ON IMPRIMITIVE SUBSTITUTION GROUPS

A THESIS

PRESENTED TO THE UNIVERSITY FACULTY OF CORNELL UNIVERSITY IN CANDIDACY FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

BY

HARRY WALDO KUHN

BALTIMORE
The Lord Baltimore Press
THE FRIEDENWALD COMPANY
1904

On Imprimitive Substitution Groups.

BY HARRY WALDO KUHN.

INTRODUCTION.

The study of substitution groups first arose in connection with the solution of algebraic equations. In the earliest work that devotes considerable attention to these groups (Ruffini, Teoria generale delle equazioni, Bologna, 1799), we find the non-cyclic groups divided into three classes which correspond to intransitive, primitive and imprimitive groups. Of the substitution groups considered in this work, the group of the order 8 and degree 4 is the only imprimitive group that receives any attention. In a memoir two years later,* Ruffini shows that the group of an irreducible equation is transitive. When the group of an equation in x is not primitive, Jordan has proved† that the equation is the result of the elimination of y from two irreducible equations of the form

$$\begin{aligned} y^m + a_1 y^{m-1} \quad + \ldots + a_m \quad &= 0, \\ x^n + b_1(y)\, x^{n-1} + \ldots + b_n(y) &= 0, \end{aligned}$$

and conversely.

The systems of imprimitivity of any imprimitive group G are permuted by its substitutions according to a transitive group P that has a $1, \alpha$ isomorphism to G, and whose degree equals the number of systems in the given set. The invariant subgroup of G that corresponds to identity in P is intransitive and its substitutions leave the given systems unchanged.‡ It is called the head of G and its order may equal unity.‖ If the group P is itself imprimitive, the corresponding systems can be united into larger ones which are permuted by the substitu-

* Memoire della società italiana delle scienze, Vol. 9, pp. 144–526. Modena, 1801.

† Traité des Substitutions, p. 259.

‡ Jordan, loc. cit., p. 41; ibid., p. 399.

‖ Dyck, Mathematische Annalen, Vol. 22 (1883), pp. 94, 108; cf. also Miller, Bulletin of American Mathematical Society, Vol. 1 (1894), p. 257.

tions of G according to a primitive group.* The degree of any solvable primitive group is the power of a prime.† In order that an equation can be solved by radicals, its group must be solvable. It follows directly that any imprimitive group that belongs to a solvable equation has at least one set of p^n systems of imprimitivity when p is a prime number.

If a given imprimitive group contains two distinct sets of systems of imprimitivity, then under certain conditions new sets of systems can be formed from these. This can always be done in case some system of the one set has more than one element in common with some system of the other set.‡ It is not true in general, however, that a new set of systems can be formed by combining all the systems of one set that have any elements in common with a given system of the other set. In his Traité des Substitutions, p. 34, Jordan states a theorem that says this can be done, but he afterwards notes the error himself.‖ Starting with this theorem he proves some very interesting results in reference to what he terms "Facteurs de Non-Primitivitat." An interesting problem presents itself here in the discussion of the imprimitive groups for which the theorem is true. An important property of such groups has recently been proved by Maillet.§

The important problem of determining when a given group can be represented as a transitive group of a given degree (or in particular as an imprimitive group) has been completely solved by Dyck.¶ When the properties of the given group are known his investigations give all the ways in which such a representation can take place. They do not determine, however, how many of the different representations of the same group are distinct as substitution groups.** This question finds its answer in a theorem due to Miller.†† In the particular case when the degree equals the order there is just one such group.

* Jordan, loc. cit., p. 399.

† Galois, Oeuvres Mathematiques, p. 27. Cf. also Jordan, l. c., p. 398.

‡ Jordan, loc. cit., p. 34.

‖ Giornale di Matematiche, Vol. 10 (1872), p. 116.

§ Bulletin de la Societé Mathématique de France, Vol. 28 (1900), p. 15.

¶ Mathematische Annalen, Vol. 22 (1883), p. 94.

** Burnside, Messenger of Mathematics, Vol. 28 (1898), p. 103.

†† Bulletin of the American Mathematical Society, 2d Series, Vol. 3 (1896), p. 215. Cf. also Giornale di Matematiche, Vol. 38 (1900), pp. 1-9.

The investigations of Dyck just referred to determine also the different sets of systems of imprimitivity which are admitted by a given imprimitive group. In particular, when the group is regular, the number of such sets is shown to be equal to the number of subgroups (not counting identity) that are contained in the group. It is clear that any substitution that is commutative with all the substitutions of a given imprimitive group determines systems of imprimitivity of the group. The number of such substitutions for any regular group is well known to be equal to the order of the group.*

The problem that has received the most attention recently in the study of imprimitive groups relates to the construction of such groups. The enumeration of the imprimitive groups of a given degree has been carried through degree fourteen. The methods used in forming these lists have been chiefly of a tentative nature. Recently, however, some theorems have been established that are useful in the determination of imprimitive groups of certain kinds.†

Any regular group of composite order is imprimitive. The determination of the number of distinct groups of a given order has been studied from the point of view of abstract groups and from that of substitution groups. By means of the latter method the regular groups whose order is less than 48 have been constructed.‡

Some imprimitive groups which do not belong to either of the two classes just mentioned have also been enumerated. These include certain groups whose orders are of a particular form. The orders that have been considered are 1) $p \cdot q \cdot \gamma$‖; 2) p_3§; and 3) $8p$¶, when p, q and γ are distinct prime numbers. Another important class of transitive groups that has been studied is formed by the groups which are isomorphic to the symmetric and the alternating groups of a given degree.** The necessary and sufficient condition that a group is multiply isomorphic to a non-regular transitive group has also been determined.††

* Jordan, Journal de l'École Polytechnique, Vol. 22 (1861), p. 153.

† For full references to those through degree 10 cf. Miller, Bulletin of the American Mathematical Society, Vol. 2 (1895), pp. 138–145. Those of degree 12 and 14 are determined by Miller, Quarterly Journal of Mathematics, Vol. 28 (1895), p. 193, and Vol. 29 (1897), p. 224. Cf. also American Journal of Mathematics, Vol. 21 (1899), p. 287.

‡ Ibid., Quarterly Journal of Mathematics, Vol. 28 (1895), p. 232.

‖ Ibid., Bulletin of the American Mathematical Society, Vol. 2 (1886), pp. 218–222.

§ Ibid., Annals of Mathematics, Vol. 10 (1896), pp. 156–8.

¶ Ibid., Philosophical Magazine (5), 43 (1896), pp. 117–125; cf. Cayley.

** Maillet, Journal de Mathématiques, 5 série, Vol. 1 (1895), pp. 5–34.

†† Miller, Giornale di Matematiche, Vol. 38 (1900), p. 8.

In the preparation of the following paper I am indebted to Dr. Miller for helpful suggestions and criticisms.

The first section of the paper relates to the imprimitive groups whose elements can be divided into systems of imprimitivity in more than one way and whose substitutions permute all the sets of systems according to primitive groups. A few properties of the heads of such groups are first given. These are followed by the study of the groups that contain a given number of heads. Those that contain more than two heads, all different from identity, receive the most attention. The cases for which one or more of the heads reduces to identity are then considered. A theorem is also given that relates to the holomorph of an abelian group of order p^m and type $(1, 1, \ldots, 1)$.

The second section considers the substitutions which are commutative with each substitution of a given transitive group. Jordan's theorem on the number of substitutions that are commutative with each substitution of any regular group is generalized so as to apply to any transitive group.

Section III relates to the construction of the imprimitive groups whose substitutions permute the systems of intransitivity of the heads according to the metacyclic group of degree p or to one of its transitive subgroups of degree p. The heads considered are: 1), those whose transitive constituents are the symmetric or the alternating groups of degree $n\,(n > 2)$, and 2), those whose constituents are transitive subgroups of degree q having a given index under metacyclic groups of the same degree.

In section IV the results of section III are made use of to determine the imprimitive groups of degree fifteen.

SECTION I.—*On the imprimitive groups whose substitutions permute all their sets of systems of imprimitivity according to primitive groups.*

1. Let G denote an imprimitive group that has more than one set of systems of imprimitivity, and let the corresponding heads of G be denoted by H_1, H_2, etc. Suppose, further, that the systems that correspond to the head H_i are permuted by the substitutions of G according to the group P_i, where i equals $1, 2, \ldots$

THEOREM.—*If the heads H_1, H_2, $\ldots$ are all different from identity, and if the groups P_1, P_2, $\ldots$ are primitive, then*

(a). *The heads can have no substitutions in common besides identity, and hence*

(b). *Each substitution of H_i is commutative with each substitution of H_j (i and j being any two of the subscripts of the H's).*

(c). *Each head contains at least one substitution whose degree equals the degree of G.*

(d). *Any head H_i is formed by establishing a one-to-one isomorphism between its transitive constituents.*

(a). The systems of intransitivity of any head of an imprimitive group are systems of imprimitivity of this group, and they are permuted by its substitutions according to a fixed transitive group. It follows that the systems of imprimitivity of the groups we are considering must be the systems of intransitivity of the heads.* Consider now any two of the heads, H_1, H_2 say. It results directly from what has been stated that H_1 and H_2 cannot consist of the same substitutions.

Let us assume then that H_1 is contained in H_2. In this case there must be an α, 1 isomorphism between P_1 and P_2. The elements of any transitive constituent of H_2 are composed of the elements in a definite number (m say) of the transitive constituents of H_1. Let the two sets of systems of imprimitivity be denoted by

$$a_1, a_2, \ldots, a_m;\quad b_1, b_2, \ldots, b_m;\quad c_1, c_2, \ldots, c_m;\quad \ldots$$

and

$$a\quad ,\quad b\quad ,\quad c\quad ,\ \ldots$$

those in the first row composing the elements of P_1 and those in the second row the elements of P_2. The subgroup h_α of order α in P_1 that corresponds to identity in P_2 can only permute the a's among each other, the b's among each other, etc. That is, h_α is intransitive, and hence P_1 is imprimitive.

Assume next that H_1 and H_2 have a common subgroup H_{12}. This group, H_{12}, is intransitive, and since it is contained in both H_1 and H_2, it is invariant in G. Its systems of intransitivity are then systems of imprimitivity. These systems, which are different from those of H_1 or H_2, are permuted by the substitutions of G according to some transitive group P. As H_{12} is contained in H_1 and H_2, the preceding argument shows that P is imprimitive. Hence, our proof of (a) is complete.

---

* Miller, American Journal of Mathematics, Vol. 21 (1899), p. 305.

(b). That each substitution of H_i is commutative with each substitution of H_j (i and j being any two of the subscripts of the H's) follows at once from the theorem: If every operator of a group G_1 transforms the group G_2 into itself, and every operator of G_2 transforms G_1 into itself, then when G_1 and G_2 have only identity in common every operator of G_1 is commutative with every operator of G_2.*

(c). Let g, h_i and p_i be the orders of G, H_i and P_i respectively; let, further

$$1,\ S_2,\ S_3,\ \ldots\ldots,\ S_g$$

be the substitutions of G, and

$$1,\ S_2,\ S_3,\ \ldots\ldots,\ S_{h_1}$$

be those of H_1. Form the rectangular array

$$\begin{array}{llll} 1, & S_2, & \ldots\ldots, & S_{h_1}, \\ S_{h_1+1}, & S_2 S_{h_1+1}, & \ldots\ldots, & S_{h_1} S_{h_1+1}, \\ \vdots & \vdots & \ldots\ldots, & \vdots \end{array}$$

from the substitutions of G. None of the rows in this array can contain more than one substitution that belongs to any head different from H_1. For if there were two substitutions in any row that belong to H_2 (say), then the inverse of one of them multiplied by the other would give a substitution, different from identity, that belongs to both H_1 and H_2. This, however, cannot be true from what has just been proved. Further, to each row there corresponds one substitution of the group P_1. Hence, it follows that any head that differs from H_1 is simply isomorphic either to P_1 or to some invariant subgroup of P_1. Now an invariant subgroup of a primitive group is transitive, and every transitive group contains substitutions whose degree equals the degree of the group. Hence every head different from H_1 contains substitutions whose degree equals the degree of G. Similarly, by writing the substitutions of G in rectangular array with respect to the head H_2, we see that H_1 contains substitutions whose degree equals that of G.

(d). We have seen that any head, H_2, that is different from H_1, is simply isomorphic to P_1 or to some invariant subgroup of P_1. Denote by Q_1 that subgroup of P_1 to which H_2 is simply isomorphic. We shall prove now that the transitive constituents of H_2 are simply isomorphic to Q_1. To establish this it

* Dyck, Mathematische Annalen, Vol. 22 (1883), p. 97.

is sufficient to prove that each substitution in H_2 involves elements from each of its transitive constituents. The subgroup Q_1 is transitive and so contains a substitution that puts any element into any other element. That is, H_2 contains a substitution that puts any system of H_1 into any other system. Since each substitution of H_1 is commutative with each substitution of H_2, it follows therefore that each substitution of H_1 contains elements from each of its transitive constituents. Similarly, each substitution of H_2 contains elements from each of its transitive constituents, and hence each constituent of H_2 is simply isomorphic to Q_1.

2. Let h_i denote the order of the head H_i.

THEOREM.—*If the order of G is equal to $h_1 h_2$, and if H_1 and H_2 are the only heads that differ from identity, then when P_1, P_2, ... are primitive groups, G has just two sets of systems of imprimitivity.*

From the argument used in proving the theorem in paragraph 1, it is clear that H_1 and H_2 can have no substitutions in common besides identity, and hence that every substitution of H_1 is commutative with every substitution of H_2. It follows that G is the direct product of H_1 and H_2. We are to prove that G can have no set of systems of imprimitivity that are interchanged by its substitutions according to a simply isomorphic primitive group.

If G has such a set of systems, it must be possible to represent it as a primitive group. It follows therefore that H_1 and H_2 must be simply isomorphic simple groups of composite order and that G, when so represented, is of degree h_1.* The subgroup G_1 of G that gives rise to its representation in the primitive form is formed by establishing a simple isomorphism between H_1 and H_2. Let the substitutions of G be denoted by the symbols

$$1,\ S_2,\ S_3,\ \ldots .,\ S_{h_1^2}$$

and let them be written in rectangular array with respect to the substitutions of G_1. If the first h_1 of the above substitutions form the subgroup G_1, we have the arrangement

$$\begin{array}{lllll}
1, & S_2 & , \ldots ., & S_{h_1}, & A_1, \\
S_{h_1+1}, & S_2 S_{h_1+1}, & \ldots ., & S_{h_1} S_{h_1+1}, & A_2, \\
 & & \ldots . & & \\
 & & \ldots . & & \\
S_{2h_1-1}, & S_2 S_{2h_1-1}, & \ldots ., & S_{h_1} S_{2h_1-1}, & A_{h_1}.
\end{array}$$

* Burnside, Theory of Groups of Finite Order, p. 190; Miller, Transactions of the American Mathematical Society, Vol. 1 (1900), p. 70.

Denote the i^{th} row of this array by A_i where $i = 1, 2, \ldots, h_1$. The symbols A may be taken for the elements of G when represented in the primitive form. Also to each element A_i there corresponds a certain number of the elements of G. That is, the subgroup G_2 of G that gives rise to its representation in the given imprimitive form must be some subgroup of G_1. The subgroup G_2 must in fact be maximal in G_1; otherwise G would contain a set of systems of imprimitivity that is permuted by its substitutions according to an imprimitive group. Since G_2 is formed by establishing a simple isomorphism between two subgroups of H_1 and H_2, it follows that G_2 is contained in a subgroup M_1 whose order is the square of its order. It is also contained in a subgroup M_2 whose order is h_1 times its order and which contains M_1. It follows that one of the corresponding sets of systems is permuted by the substitutions of G according to an imprimitive group. Hence G has just two sets of systems of imprimitivity.

3. THEOREM.— *When G is regular and has just two heads that differ from identity, then if $P_1, P_2, \ldots$ are primitive groups, G is the cyclic group of order pq where p and q are distinct primes.*

The number of sets of systems that belongs to any regular group is equal to the number of its subgroups, not including identity or the whole group.* Hence the two heads that differ from identity must be generated by substitutions of prime order and the order of one must be different from that of the other.

4. THEOREM.—*If G contains more than two sets of systems of imprimitivity, and if $H_1, H_2, \ldots$ are all different from identity, then when $P_1, P_2, \ldots$ are primitive groups,*

(a). *The degree of any substitution besides identity of each head is equal to the degree of G.*

(b). *The heads are simply isomorphic abelian groups; each is of degree p^{2m} of order p^m and of type $(1, 1, \ldots, 1)$ where p is a prime and m is a positive integer.*

(a). We prove first that in any such group the heads can contain, besides

---

* Dyck, Mathematische Annalen, Vol. 22 (1883), p. 89.

identity, only substitutions whose degree equals that of G. As in the theorem of paragraph 1, write the substitutions of G in rectangular array with respect to the substitutions of H_1. We know that any other head is simply isomorphic to P_1 or to some invariant subgroup of P_1. Consider the two heads H_2 and H_3 and let Q_2 and Q_3 denote the respective subgroups of P_1 to which these heads are simply isomorphic. Both Q_2 and Q_3 contain substitutions whose degree equals the degree of P_1, since an invariant subgroup of a primitive group is transitive. Further, neither Q_2 nor Q_3 can contain a substitution whose degree is less than that of P_1. This may be seen as follows: Each substitution of Q_2 is commutative with each substitution of Q_3, since the heads of H_2 and H_3 have this property. Suppose now that Q_3 contains a substitution S whose degree is less than that of P_1. Then the group $\{Q_2, S\}$ that is generated by Q_2 and S is transitive since Q_2 is transitive. As the substitution S is commutative with each substitution of Q, this transitive group will contain an invariant substitution S whose degree is less than the degree of the group. This, however, cannot be true, since an invariant substitution of a transitive group of degree n must be regular and of degree n. It follows, therefore, that the degree of each substitution, besides identity of any head that differs from H_1, is the same as the degree of G. By writing the substitutions of G in rectangular array with respect to H_2, it follows by a similar argument that H_1 also possesses this property.

(b). The group generated by any two of the heads, H_1 and H_2 say, must be transitive. If it were intransitive it would form a new head that contains both H_1 and H_2, and this cannot be true according to theorem 1 of this section. Further, this group $\{H_1, H_2\}$ must contain the substitutions of all the heads of G. For if it did not contain a substitution S of some other head, then $\{H_1, H_2\}$ and S would generate a transitive group whose substitutions all have the same degree as that of the group and which contains a number of substitutions that is greater than this degree. This, however, cannot be true. It follows, therefore, that the heads are simply isomorphic to each other.

In the group that is generated by the substitutions of H_2 and H_3 are found the substitutions of H_1. Also any substitution of H_2 or of H_3 is commutative with each substitution of H_1, and, therefore, any substitution in the group $\{H_2, H_3\}$ is commutative with each substitution of H_1. It follows that H_1, and hence also each of the heads of G, is abelian. Further, each head must be of

order p^m (where p is a prime and m is a positive integer) and of type $(1, 1, \ldots, 1)$. For if the substitutions of the heads were not all of the same prime order, then the subgroup of $\{H_1, H_2\}$ that is generated by its substitutions of lowest order would form a head that would not satisfy the requirements of the theorem in paragraph 1. Finally, since the group $\{H_1, H_2\}$ is regular, it follows that the degree of G is p^{2m}.

Corollary: *If G is regular it must be the non-cyclic group of order p^2.*

When G is regular it must coincide with the group generated by any two of its heads. It is then an abelian group of order p^{2m} and of type $(1, 1, \ldots, 1)$. The only groups of this type that satisfy the requirements of the above theorem are clearly the groups of order p^2.

5. Let P denote an abelian group of order p^m and of type $(1, 1, \ldots, 1)$ when represented as a transitive group in the elements

$$a_1, a_2, \ldots, a_{p^m}.$$

With each substitution of P associate that element which replaces a_1 in that substitution. The group of isomorphisms of P may then be represented as a transitive group in the $p^m - 1$ elements

$$a_2, a_3, \ldots, a_p \; ;$$

when so represented, let it be denoted by R. The transitive group (h) that is generated by the two groups P and R is simply isomorphic to the holomorph of P.

Now to any subgroup of R whose degree is less than $p^m - 1$, there corresponds an imprimitive subgroup of h. For such a subgroup of R would transform some of the substitutions of P into themselves, and these would form an invariant intransitive subgroup of the corresponding subgroup of h.

Further, to any transitive subgroup (R_1) of R whose degree equals $p^m - 1$, there corresponds a primitive subgroup (h_1) of h. For R_1 is the subgroup of h_1 that leaves one of its elements fixed; since this is transitive, it follows that h_1 is primitive.

It remains to consider those intransitive subgroups (I) of R that are of degree $p^m - 1$. We note in the first place that if the subgroup (h') of h that corresponds to I is primitive, then any substitution of I besides identity must contain elements from each one of its transitive constituents. Suppose that

some of the substitutions of I that differ from identity do not contain any elements from a given one of its transitive constituents. These substitutions form an invariant subgroup (I') of I whose degree is less than $p^m - 1$. The substitutions of P that correspond to the elements of I that are not found in I', form with identity a subgroup of P. This subgroup is invariant in h', and hence the latter would be imprimitive. Hence, when h' is primitive, I must be formed by establishing a simple isomorphism among its transitive constituents. Every subgroup I of this kind that is contained in R does not give rise, however, to a primitive subgroup of the holomorph. For example, when p equals 2 and m equals 4, R contains a subgroup of order 3 and of degree 15 that gives rise to an imprimitive subgroup of order 48 in the holomorph. The substitutions of P that correspond to the elements in each transitive constituent of the given subgroup of order 3 generate subgroups of order 4. In general, it is evident that the necessary and sufficient condition that h' is primitive is that the elements of each transitive constituent of I contain a set of independent generators of P. If the substitutions that correspond to the elements of any transitive constituent of I generate a subgroup of P of order p^a where a is less than m, then this subgroup is invariant in h' and the latter is imprimitive.

Hence we have this

THEOREM.—*A subgroup (h') of the holomorph (h) of P, that corresponds to a subgroup (R_1) of the group of isomorphisms (R), is primitive*

(a). *When R_1 is a transitive subgroup of degree $p^m - 1$*, or

(b). *When R_1 is an intransitive subgroup of degree $p^m - 1$ that is formed by establishing a simple isomorphism among its transitive constituents and that is such that the elements of each of its transitive constituents contain a set of independent generators of P.*

Any other subgroup of R gives rise to an imprimitive subgroup of h.

Corollary: *When the number of elements in each transitive constituent of R is less than m, the subgroup h' is imprimitive.*

This follows at once from the above theorem, since the number of operators in a set of independent generators of P is m.

6. The theorem just stated is useful in the determination of the primitive groups of degree 16. For it is known that every primitive group of this degree

that does not include the alternating group, contains an invariant abelian subgroup of order 16 and of type (1, 1, 1, 1).*

7. By means of the two preceding theorems we can investigate the number of distinct imprimitive groups G of a given degree that have more than two sets of systems of imprimitivity (the heads differing from identity), and that have all their sets permuted according to primitive groups by the substitutions of G. Any such group is of degree p^{2m}, and the transitive constituents of any of its heads are abelian groups of order p^m and of type $(1, 1, \ldots, 1)$. Also each head is formed by establishing a one-to-one isomorphism among its transitive constituents, the number of these being p^m. Denote the transitive constituents of the head H_1 by the symbols

$$A_1, A_2, \ldots A_{p^m}.$$

It follows that P_1 is a transitive group in these symbols that contains a regular abelian group (P') of type $(1, 1, \ldots, 1)$ as an invariant subgroup. That is, P_1 must be some subgroup of the holomorph (h) of P' that contains P', h being represented as a transitive group in the symbols $A_1, A_2, \ldots, A_{p^m}$. We consider then those imprimitive groups that contain the head H_1 and whose systems of imprimitivity that are determined by H_1 are permuted according to the primitive subgroups of h that contain P'; the groups G must be found among these.

Let the substitutions of H_1 be denoted by the symbols

$$1, S_2, S_3, \ldots, S\ .$$

It is assumed that S_j replaces a_1 by a_j, and that the substitution of the constituent A_i that occurs in S_j is found by replacing the element a_k of the substitution of A_1 that occurs in it by the corresponding element of A_i, where $k = 1, 2, \ldots, p^m$ and i, j are any two of these numbers. The substitutions that interchange the transitive constituents of H_1 in the simplest way according to the substitutions of P, form a second head H_2. Let the substitutions of this head be denoted by the symbols

$$1, t_2, t_3, \ldots, t_{p^m},$$

---

* Miller, American Journal of Mathematics, Vol. 20 (1898), p. 229.

t_j being that substitution of H_2 that corresponds to the substitution of P' that replaces A_1 by A_j. Now, any third head H_3 must be formed by establishing some simple isomorphism between the substitutions of H_1 and H_2. Without loss of generality, we may assume that the substitutions of H_3 are represented by the symbols

$$1,\ S_2t_2,\ S_3t_3,\ \ldots\ldots,\ S_{p^m}t_{p^m}.$$

For let H_3' denote the group formed by establishing some other isomorphism between H_1 and H_2. A certain permutation of the symbols that denote the substitutions of H_1 will change H_3' into H_3, and corresponding to this permutation there is a definite substitution (S') in the group of isomorphisms of A_1. Let S_1' denote one of the substitutions of the holomorph of A_1 that corresponds to S' (the holomorph being represented transitively of degree p^m), and let S_i' denote the same substitution in the elements of the constituent A_i where $i=2, 3, \ldots, p^m$. Then the substitution $S_1' S_2' \ldots\ldots S_{p^m}'$ transforms H_1 and H_2 into themselves and H_3' into H_3. That is, a group that contains the heads H_1, H_2 and H_3' can be transformed into one that contains the heads H_1, H_2 and H_3.

The largest group within which H_1 is invariant without having its systems of intransitivity interchanged is the group generated by the holomorphs of each of its transitive constituents $A_1, A_2, \ldots\ldots, A_{p^m}$, these being represented as transitive groups of degree p^m. The order of the resulting group divided by p^m gives then the number of sets of substitutions of p^m each that permute according to each substitution of P_1.

When P_1 is regular, that is when G is regular, it is clear that m must equal unity. If m were greater than unity, G would contain systems of imprimitivity that are not permuted by its substitutions according to primitive groups.

When P_1 is not regular, let S' denote any substitution in P that is not contained in P'; and let t' denote the substitution that interchanges in the simplest manner the transitive constituents of H_1 according to S'. The substitution S' transforms the substitutions of P' according to a certain operator in the group of isomorphisms of P'; and t' transforms the substitutions of H_2 in exactly the same way. Further, t' is commutative with each substitution of H_1. Suppose now that any one of the substitutions which with H_1 generate the sets of substitutions that permute according to S' be denoted by

$$s_1 s_2, \ \ldots, s_{p^m} t', \tag{A}$$

where s_i is some substitution in the holomorph of A_i, i being any of the numbers $1, 2, \ldots, p^m$. Since the substitution (A) must transform H_2 into itself, it follows that

$$s_1 s_2, \ldots, s_{p^m} \tag{B}$$

must be commutative with each of the substitutions t_i, where i is as above. Hence s_i must be the same substitution in the elements of A_i as s_j is in the elements of A_j, i and j being any two of the numbers $1, 2, \ldots, p^m$. The number of substitutions (B) is then not greater than the number of operators in the group of isomorphisms of A_1. Further, since (A) must transform H_3 into itself, it follows that the substitution (B) must transform the substitutions of H_1 in exactly the same way as t' transforms the substitutions of H_2. That is, (B) is a fixed substitution. It is clear also that the corresponding substitution (A) thus found has its proper power in the head H_1. Hence there is one and only one generating substitution that permutes according to S' that transforms H_1, H_2 and H_3 into themselves respectively, and that has its proper power in H_1. That is, there is just one imprimitive group of the given kind that is isomorphic to any primitive group P_1. The number of primitive groups that contain P' is given by the preceding theorem, so that we have determined now the number of imprimitive groups G of degree p^{2m}. Of the groups G thus found, it is evident that to conjugate subgroups (R_1) of the group of isomorphisms correspond conjugate groups G. We have then the

THEOREM.—*The number of imprimitive groups G of a given degree that contain more than two sets of systems of imprimitivity (the heads differing from identity) and for which P_1, P_2, ... are primitive groups, is as follows:*

(a). *When G is regular, there is just one such group; its degree is p^2.*

(b). *When G is not regular, the number is equal to the number of distinct primitive groups that are contained in the holomorph (h) of the abelian group P' and that contain P'.*

It is well known that the group of isomorphisms of an abelian group of order p^m and of type $(1, 1, \ldots, 1)$ is simply isomorphic to the linear homogeneous group.* It appears then that the study of the imprimitive group G of the above theorem is closely associated with that of the linear homogeneous group.

* Moore, Bulletin of the American Mathematical Society, Vol. 2 (1895), p. 34.

8. We proceed now to investigate the number of sets of systems of imprimitivity that belong to the groups just determined. When G is regular, it is the non-cyclic group of order p^2 and so contains $p+1$ sets of systems—this being the number of subgroups differing from identity that G contains.

Suppose then that G is a non-regular group. Let R_1 denote the subgroup of P_1 that leaves any element fixed. We note first that G does not admit the head identity. The subgroup (G_1) of G that leaves any element fixed has one and just one substitution in common with any division of G—the divisions being formed with respect to the subgroup that contains the heads $H_1, H_2, \ldots.$ If now G admits the head identity, then G_1 must be contained in a larger subgroup of G which contains no invariant subgroup of G. This is evidently not the case. Any head of G that differs from H_1 and H_2 is then formed by establishing some simple isomorphism between these two heads. Denote by H_4 any such isomorphisms that differ from H_3. Our problem is to determine under what conditions H_4 will be transformed into itself by the substitutions of G. Corresponding to H_4 there is a definite isomorphism of H_2 to itself, viz., the one formed by replacing each S in H_4 by the corresponding t. And this again corresponds to a definite isomorphism of P' to itself. That is, to H_4 there is associated in this way a definite substitution (r) of the group of isomorphisms of P'. Also when H_4 is transformed into itself by the substitution of G, it is clear that r must be transformed into itself by the substitutions of R_1; and conversely. It follows, therefore, that the number of heads H_4 is equal to the number of substitutions differing from identity in the group of isomorphisms of P' that are commutative to each substitution of R_1. To identity corresponds the head H_3. Hence the

THEOREM.—*The number of sets of systems of imprimitivity of the groups G in the preceding theorem is as follows:*

(a). *When G is regular, there are* $p+1$ *different sets.*

(b). *When G is non-regular, there are* $c+2$ *different sets, where c is the number of substitutions in the group of isomorphisms of* P' *that are commutative with each substitution of* R_1.

9. We consider now the imprimitive groups G that contain more than one set of systems of imprimitivity, each set being permuted by the substitutions of

G according to a primitive group, and that have all their heads identity except one.

Suppose in the first place that G denotes a regular group of this kind. We know that every regular group contains a set of systems of imprimitivity that is permuted by its substitutions according to any transitive representation of the group. It follows then that G must be a group that can be represented in the imprimitive form only when its degree equals its order, and that can be represented in the primitive form of a lower degree. The only groups that satisfy these requirements are the non-cyclic groups of order pq, where p and q are distinct primes.* If $p > q$, these groups contain $q + 1$ subgroups, not including identity and hence G contains $q + 1$ sets of systems of imprimitivity. The heads that correspond to q of these are identity and the remaining head is of order p. Hence we have the

THEOREM.—*The only regular groups G that contain more than one set of systems of imprimitivity, each set being permuted by the substitutions of G according to a primitive group, and that have only one head different from identity, are the non-cyclic groups of order pq, where p and q are distinct primes. If $p > q$, these groups have $q + 1$ sets of systems of imprimitivity.*

10. Suppose next that the subgroup (G_1) of G that leaves one element fixed is contained in the head (H) that differs from identity. When G_1 is of order unity, the groups G are determined by the preceding theorem. Also when G is regular, the subgroup G_1 is maximal in H. We prove now that this is true when G is non-regular.

If G_1 is not maximal in H, there is a subgroup H_1 of H in which G_1 is maximal. This subgroup H_1 determines a set of systems of imprimitivity of G. Two cases arise according as H_1 contains an invariant subgroup of G or does not contain such a subgroup. In the former case the set of systems that corresponds to H_1 is left unchanged by the substitutions of the invariant subgroup contained in H_1. The group G would contain then two heads that differ from identity; this is contrary to the assumption made. In the latter case the set of systems that corresponds to H_1 is permuted by the substitutions of G according to a group (P)

* Dyck, Mathematische Annalen, Vol. 22 (1883), p. 101.

that is simply isomorphic to G. Since H_1 is not maximal in G, the group P would be imprimitive. It follows, therefore, that G_1 is a maximal subgroup of H.

Suppose now that H is contained in a subgroup (H') of G whose order exceeds that of H. The subgroup H' gives rise to a set of systems of imprimitivity that are found by uniting the systems that correspond to H into larger systems. This new set of systems is left unchanged by the substitutions of H, and so in this case G contains two heads that differ from identity. It follows accordingly that H is a maximal subgroup of G. That is, the quotient group G/H is of prime order p.

The systems of imprimitivity that are left unchanged by H are permuted by the substitutions of G according to a primitive group that is simply isomorphic to the quotient group G/H. Since these systems are the systems of intransitivity of H, it follows that the number of transitive constituents of H is equal to p.

Consider now a set of systems that is not left unchanged by any substitution of G besides identity, and let P denote the primitive group according to which this set of systems is permuted by the substitutions of G. The subgroup P' of P that corresponds to the subgroup H of G is transitive. Suppose now that H is not formed by establishing a simple isomorphism among its transitive constituents. It contains then an invariant subgroup whose degree is less than the degree of H. The subgroup of P' that corresponds to this invariant subgroup of H would be of a lower degree than the degree of P; also it would be invariant in P'. This, however, cannot be true, since an invariant subgroup of a transitive group is of the same degree as that of the group. Hence H is formed by establishing a simple isomorphism among its transitive constituents.

The subgroup of G that gives rise to the primitive representation P just considered, must contain G_1 as an invariant subgroup, and its order is equal to pg_1, where g_1 is the order of G_1. Its order could not be greater than pg_1 since then G_1 would not be maximal in H. It follows that the degree of P is equal to the degree of each of the transitive constituents of H, so that to each element of P there are associated p elements of G. Also since G_1 is maximal in H, it follows that P' is a primitive group.

When G is not regular, there is just one subgroup besides H that contains G_1. That is, there is just one set of systems that is permuted by the substitu-

tions of G according to a simply isomorphic group. It follows, therefore, that when G is not regular, it contains just two sets of systems of imprimitivity.

These results may be summed up in the

THEOREM.—*If G denotes an imprimitive group having more than one set of systems of imprimitivity, each set being permuted according to a primitive group by the substitutions of G, and if just one of the heads (H) differs from identity, then when the subgroup (G_1) of G that leaves any element fixed, is contained in H.*

(a). *The head H is maximal in G, the quotient group G/H being of prime order p. Also H is formed by establishing a simple isomorphism among its transitive constituents—the number of these being p.*

(b). *The subgroup G_1 is maximal in H.*

(c). *G has just two sets of systems when it is not regular. The one whose head is identity contains p elements in each system.*

11. It is not difficult to construct general classes of groups that come under those defined in the preceding theorem.

Suppose, for example, that the transitive constituents of H are alternating groups of degree $n\,(n > 2)$ and that H is formed by writing after each substitution of the first constituent the same substitution in the other constituent. H has just two transitive constituents. A substitution which with H generates a group G of the kind in question cannot be the ordinary t; for this would be a commutative substitution and the resulting group could not be represented in primitive form. Let s_1 denote any negative substitution of the symmetric group of degree n that contains the first transitive constituent of H; and let s_2 denote the same substitution in the elements of the second constituent. Then

$$s_1 s_2 t \tag{A}$$

is a substitution which with H generates a group G of the desired kind. Further, there is just one group of this kind. For any other substitution that could be used in place of (A) would be of the form

$$s_1 S_2 s_2 t\,,$$

where S_2 is some substitution in the elements of the second constituent that is commutative with each substitution of this constituent. Since the constituents are primitive groups there is no such substitution except when $n = 3$. In this latter case the group is regular and there is just one.

A second class of groups G is obtained in a similar way if we take for the transitive constituents of H semi-metacyclic groups of degree q. The groups thus obtained are of degree $2q$, and they are simply isomorphic to the metacyclic groups of degree q.

12. Let, finally, G denote an imprimitive group that contains no head that differs from identity and that has all its sets of systems of imprimitivity permuted by its substitutions according to primitive groups. Denote by G_1 the subgroup that leaves a given element unchanged.

The simple group of order 60, when represented as a transitive group of degree 12, illustrates the occurrence of a group of this kind that has just one set of systems. When the same group is represented as a transitive group of degree 20, it has two sets of systems, both of which are permuted according to primitive groups. In these examples the subgroup G_1 is maximal in larger subgroups of G. In general, it is evident that *the subgroup G_1 must be maximal in any larger subgroup (G_2) of G in which it is found, and, further, that the subgroup G_2 cannot contain any invariant subgroup of G besides identity.* It is clear that G cannot be regular. Also its order cannot be the power of a prime. The number of sets of systems that belong to any such group is equal to the number of subgroups G_2 that it contains.

13. THEOREM.—*Every imprimitive group G that admits only the heads identity is insolvable.*

Since G admits only identity as a head, it must be possible to represent it as a primitive group (P). If now G is solvable, so also is P. Suppose that G is solvable. Then P must be of degree p^a, where p is a prime, and it contains as a minimal invariant subgroup an abelian group (P_1) of order p^a and type $(1, 1, \ldots, 1)$.* To the subgroup P_1 of P there corresponds an invariant subgroup of G; and since P_1 is regular and of degree p^a, it follows that this subgroup is also intransitive. Hence G in this case contains a head that differs from identity, and this contradicts our hypothesis.

* Galois, Oeuvres Mathématiques, p. 27. Cf. also Jordan, Traité des Substitutions, p. 398.

SECTION II.—*The substitutions which are commutative with each substitution of any transitive group.*

1. THEOREM.—*Let G denote any transitive group of degree n and order g. The number of substitutions in the elements of G that are commutative with each of its substitutions is equal to the order of the quotient group H/G_1, where G_1 is a subgroup of G that leaves any element fixed, and H is the largest subgroup of G that contains G_1 self-conjugately.*

It is well known that this theorem is true when G is regular.* To prove that it is true for any transitive group G, let the substitutions of the group be denoted by

$$1,\ S_2,\ S_3,\ \ldots\ldots,\ S_g,$$

and the elements of these substitutions by

$$a_1,\ a_2,\ \ldots\ldots,\ a_n.$$

Suppose that G_1 is that subgroup of G which leaves a_1 fixed, and let its substitutions be denoted by

$$1,\ S_2,\ S_3,\ \ldots\ldots,\ S_{g_1},$$

where g_1 is the order of G_1.

The substitutions of G may be arranged in the following rectangular array:

$$\left.\begin{array}{llcll} 1 & ,\ S_2 & ,\ \ldots\ldots, & S_{g_1} & ,\ a_1, \\ S_{g_1+1} & ,\ S_2S_{g_1+1} & ,\ \ldots\ldots, & S_{g_1}S_{g_1+1} & ,\ a_2, \\ & & \ldots\ldots & & \\ S_{g_1+n-1}, & S_2S_{g_1+n-1}, & \ldots\ldots, & S_{g_1}S_{g_1+n-1}, & a_n. \end{array}\right\} \qquad \text{I}$$

In this array the substitutions of the i^{th} row replace a_1 by a_i where i is any of the numbers $1, 2, \ldots\ldots, n$. Also if the i^{th} row is denoted by a_i, then any substitution S_x of G is given by the permutation on the symbols associated with the rows which arises when all the substitutions of the array are multiplied by S_x.† If the substitution S_x is commutative with each substitution of G, then evidently the same permutation of the rows will take place whether pre-multiplication or post-multiplication is made use of.

* Jordan, Journal de l'École Polytechnique, Vol. 22 (1861), p. 158; cf. Traité des Substitutions, p. 60.
† Miller, Bulletin of the American Mathematical Society, 2d series, Vol. 3 (1896), p. 214.

We prove now that any substitution C, which is not found in G and which is commutative to each of the substitutions of G, is given by the permutation on the symbols associated with the rows that arises when some substitution of G is multiplied by all its substitutions, i. e., by pre-multiplication of some substitution of G. Since C is not found in G, it will generate with G a larger transitive group G' in the same elements. The subgroup G_1' of G' that leaves a_1 fixed will contain G_1. Let $S_t C$ denote a substitution which with G_1 will generate G_1', S_t being some substitution of G. As above, the substitutions of G' may be arranged in the following array:

$$\left.\begin{array}{llllllll} 1 & , S_2 & , \ldots, & S_{g_1} & , & S_t C & , \ldots, & a_1, \\ S_{g_1+1} & , S_2 S_{g_1+1} & , \ldots, & S_{g_1} S_{g_1+1} & , & S_t C S_{g_1+1} & , \ldots, & a_2, \\ \vdots & & \ldots & & & & \ldots & \\ S_{g_1+n-1}, & S_2 S_{g_1+n-1}, & \ldots, & S_{g_1} S_{g_1+n-1}, & & S_t C S_{g_1+n-1}, & \ldots, & a_n. \end{array}\right\} \quad \text{II}$$

The substitution C is contained in this array, and, as noted above, if the pre-multiplication of C upon the substitutions of G is performed, the resulting permutation on the elements denoting the rows is identical with C. If pre-multiplication be used with reference to any substitution in the first row of the array, then each row goes into itself. This follows at once from the fact that tthe substitutions in the i^{th} row replace a_1 by a_i, where i equals $1, 2, \ldots, n$.

Suppose now that the substitution $S_t^{-1} C^{-1} C$ is multiplied by each substitution of G'. From what has just been said, it follows that the resulting permutation on the letters associated with the rows is identical with C. The substitution $S_t^{-1} C^{-1} C$ is identical with S_t^{-1}, and hence we have proved our statement.

We prove now that the number of substitutions of G which by pre-multiplication give rise to distinct permutations on the elements associated with the rows of the array I, is equal to the order of the quotient group H/G_1, where H is the largest group that contains G_1 self-conjugately. Let $S_t G_1$ and $G_1 S_t$ denote the result of pre-multiplication and post-multiplication of G_1 with S_t respectively. Then if S_t by pre-multiplication gives rise to a permutation C of the rows of I, we must have

$$S_t G_1 \equiv G_1 S_{g_1+k},$$

$$\therefore \qquad S_t G_1 S_t^{-1} \equiv G_1 S_{g_1+k} S_t^{-1} \equiv G_1 S_r, \qquad (S_r = S_{g_1+k} S_t^{-1}).$$

The right-hand member of this identity consists of the substitutions found in some row. And since the left-hand member contains the identical substitution, it follows that S_t must transform G_1 into itself. Conversely, if S_t transforms G_1 into itself, it gives rise to a permutation of the rows of I.

It has been seen above that, if S_t is a substitution of G_1, the corresponding substitution C is the identical substitution. When S_t is any substitution of H that is not found in G_1, the corresponding substitution C will be different from identity. Also all the substitutions of H that are found in the same row with S_t will give rise to the same substitutions C, since these substitutions are found by multiplying those of G_1 by S_t.

Finally, the substitutions C that correspond to substitutions S_t that are found in different rows of H are distinct. For each replaces a_1 by the element associated with the row in which it is found. The number of substitutions C is then equal to h, the order of the quotient group H/G_1. It is clear also that the substitutions found in this way are all commutative with each substitution of G.

Since H is a subgroup of G, it follows that the number of rows contained in H is a divisor of the number contained in G. Hence

Corollary I.—*The number of substitutions that are commutative with each substitution of G is equal to some divisor of the degree of G.*

When G is a primitive group, the subgroup G_1 that leaves one element fixed, is maximal, and in this case the order (h) of H/G_1 is equal either to unity or to g. Hence we have

Corollary II.—*Identity is the only substitution that is commutative with each substitution of a primitive group of composite order.*

2. If α denotes the number of letters left fixed by G_1, then n/α is the number of subgroups in the conjugate set to which G_1 belongs. The number of substitutions, x, that transform G_1 into itself is the same as the number that transforms it into any one of its conjugates.

$$\therefore \qquad x \,.\, n/\alpha = g = ng_1,$$

or

$$x = \alpha g_1,$$

or

$$x/g_1 = h = \alpha.$$

The above theorem may therefore be stated in this form:

The number of substitutions in the elements of any transitive group G that are commutative with each of its substitutions is equal to the number of elements that are left unchanged by the subgroup G_1 that leaves any element of G unchanged.

When the order of G is the power of a prime, then the order of the quotient group H/G_1 is also the power of the same prime. Hence we have

Corollary I.*—*If the order of G is the power of a prime, then the number of elements left unchanged by G_1 is a power > 1 of the same prime.*

3. When G is a regular group, the substitutions that are commutative with each of its substitutions, form a group that is simply isomorphic to G. So in this case the order of each substitution that is commutative to all the substitutions of G is equal to the order of some substitution of G. When G is not regular, this is still true. For, from the method of forming any substitution C that is commutative to all the substitutions of G, it follows that to C there corresponds a definite substitution in the associate of G whose order equals that of C. We have then the

THEOREM.—*The order of any substitution that is commutative with each substitution of a transitive group is equal to the order of some substitution of that group.*

4. Let the associate of a group G whose order is g be denoted by G'. If G contains no invariant substitution, then it contains no substitutions in common with G. In this case G and G' generate a group $\{G, G'\}$ whose order equals g^2 and whose degree equals g. *The subgroup G_1 that leaves any element fixed in $\{G, G'\}$, is formed by establishing some simple isomorphism between G and G'.*

For, suppose the substitutions of $\{G, G'\}$ are written in rectangular array in such a way that the substitutions of G form the first row. The subgroup G_1 cannot have more than one substitution in common with any row of this array. If it had two, then one times the inverse of the other would belong to G, and this could not be true since this product would be a substitution differing from identity that is found in G. The group G_1 contains, therefore, just one substitution from each row of our array. The substitutions in any row are found by multiplying the g substitutions of G by some substitution of G'. Further, no

* Miller, American Journal of Mathematics, Vol. 28 (1900), p. 178.

two substitutions of G_1 can involve the same substitution of G; for then one times the inverse of the other would be of degree g. It follows directly that G_1 consists of a simple isomorphism between G and G'.

5. By means of the statement just proved in reference to G_1, we can give an easy proof by substitution theory of the fundamental theorem that every group whose order is the power of a prime, contains invariant substitutions. Suppose that such a group G of order p^a does not contain any invariant substitution. Then $\{G, G'\}$ is of order p^{2a}, and G_1 is formed by establishing some simple isomorphism between G and G'. The subgroup G_1 in this case leaves a multiple of p elements fixed and so is transformed into itself by some substitution S of G. This substitution S is commutative with each substitution of G', and hence must also be commutative with each substitution of G. It follows that our hypothesis is wrong, and so G contains invariant substitutions.

SECTION III.—*Some theorems relating to the construction of imprimitive groups.*

1. In constructing the imprimitive groups of a given degree by means of tentative processes, the number of trials that needs to be made is frequently large, and much of the work is merely repetition. Further, it frequently happens that the method by means of which certain groups of a given degree can be found, needs little change to determine corresponding groups of other degrees. It seems desirable then to establish general theorems which apply to groups of different degrees. Several theorems of this nature have already been proved.* Of these, one of the most useful states that "there is only one imprimitive group whose head is the product of the groups obtained by writing a given group in the different systems of elements, and which permutes the systems according to a given cyclical substitution."

The theorems in paragraph 2 to 7 will be found useful in constructing the imprimitive groups of degree np, where n is any integer greater than 2, and p any prime number. Let G' denote the symmetric group in the elements $a_1, a_2, \ldots, a_n$; G'', the symmetric group in the elements $b_1, b_2, \ldots, b_n$; $\ldots$; G^p, the sym-

* Miller, Quarterly Journal of Mathematics, Vol. 28 (1895), p. 193; American Journal of Mathematics, Vol. 21 (1899), p. 295.

metric group in the elements $m_1, m_2, \ldots, m_n$. Also let P denote the metacyclic group of degree p in the letters $A, B, C, \ldots, M$ and P_{i_2} that invariant subgroup of P whose index under P is i_2. When i_2 is different from $p-1$, the group P_{i_2} may be generated by a substitution (p_1) of order p and a substitution (p_2) of order $\frac{p-1}{i_2}$; when i_2 equals $p-1$, the group P_{i_2} is generated by a single substitution of order p. The generator p_1 may be taken as the substitution $ABC \ldots M$, and it may be assumed that the generator p_2 does not contain the letter A. When p equals 2, P will denote the group (AB). The substitutions that permute the systems in the simplest way according to p_1 and p_2 will be denoted by t_1 and t_2 respectively. That is,

$$t_1 \equiv a_1b_1c_1 \ldots m_1 . a_2b_2c_2 \ldots m_2 . \ldots . a_nb_nc_n \ldots m_n,$$

and t_2 is a substitution of order $\frac{p-1}{i_2}$ that does not involve the elements $a_1, a_2, \ldots, a_n$.

2. THEOREM.—*The number of imprimitive groups of degree np that contain the head*

$$H \equiv \{G', G'', \ldots, G^p\} \text{ pos*}$$

and whose substitutions permute the systems of intransitivity of H according to P_{i_2} is as follows:

(a). *When $p = 2$, there are two such groups.*

(b). *When $p > 2$, there is one group if $\frac{p-1}{i_2}$ is odd and two groups if $\frac{p-1}{i_2}$ is even.*

The largest group within which the given head is invariant without having its systems of intransitivity interchanged is $\{G', G'', \ldots, G^p\}$. Hence there are just two sets of substitutions that transform according to any substitution of P_{i_2}. Those that permute according to p_1 may be obtained by multiplying the substitutions in the head by

$$t_1 \text{ and } a_1a_2 . t_1.$$

---

* The notation used is that given by Cayley, Quarterly Journal of Mathematics, Vol. 25 (1890–1), p. 71.

Both of these transform H into itself. The p^{th} power of t_1 is identity, while that of $a_1a_2 . t_1$ is $a_1a_2 . b_1b_2 \ldots . m_1m_2$. This latter is found in the head only when $p = 2$. Hence there is just one imprimitive group that contains the given head and that corresponds to P_{p-1} when $p > 2$. When $p = 2$, there are two such groups; these are distinct, since one contains negative substitutions while the other does not.

When i_2 is less than $p-1$, the substitutions that permute according to p_2 may be obtained by multiplying the substitutions of H by

$$t_2 \text{ and } a_1a_2 . t_2 .$$

Since there is just one group that corresponds to P_{p-1}, each group that corresponds to P_{i_2} must contain this, and hence we may assume that t_1 is found in each such group. The substitutions t_2 and $a_1a_2 . t_2$ both transform the head and also the group that corresponds to P_{p-1} into themselves. The $\frac{p-1}{i_2}$th power of t_2 is identity, and hence there is always one group that corresponds to P_{i_2}. The $\frac{p-1}{i_2}$th power of $a_1a_2 . t_2$ is identity or a_1a_2 according as $\frac{p-1}{i_2}$ is even or odd. Hence $a_1a_2 . t_2$ may be used only when $\frac{p-1}{i_2}$ is even. The corresponding group is distinct from the one obtained when t_2 is taken, as the one contains negative substitutions while the other does not. Hence, when $\frac{p-1}{i_2}$ is even there are two groups that correspond to P_{i_2}, and when $\frac{p-1}{i_2}$ is odd there is just one such group.

3. THEOREM.—*When* $p > 2$, *there is just one imprimitive group of degree* np *that contains the head*

$$H \equiv G' \text{ pos } G'' \text{ pos } \ldots . \, G^p \text{ pos } + G' \text{ neg } G'' \text{ neg } \ldots . \, G^p \text{ neg}$$

and whose substitutions interchange the systems of intransitivity of H *according to* P_{i_2}. *When* $p = 2$, *there are two such groups.*

The largest group within which H is invariant without having its systems interchanged is $\{G', G'', \ldots . , G^p\}$, and hence there are 2^{p-1} sets of substitutions that transform according to a given substitution of P_{i_2}, The 2^{p-1} sets

that transform according to p_1, may be found from H and the substitutions obtained by multiplying each substitution in the group

$$(s_1)(s_2) \ldots\ldots (s_{p-1}) \tag{A}$$

by t_1, where $s_1 = a_1a_2$, $s_2 = b_1b_2$, etc. Each of these transforms H into itself and each has its p^{th} power in H. The resulting groups, however, are all conjugate when p is greater than 2. For

$$s_3s_5 \ldots\ldots s_pt_1s_3s_5 \ldots\ldots s_p = s_1s_3 \ldots\ldots s_pt_1.$$

That is, the group $\{H, t_1\}$ can be transformed into the group $\{H, s_1t_1\}$. Similarly, it can be transformed into the groups $\{H, s_it_1\}$, where $i = 2, 3, \ldots\ldots, p-1$ and, therefore, into all the others. Hence when $p > 2$, there is just one group that corresponds to P_{p-1}. It may be taken as $\{H, t_1\}$, and we may assume that it is found in each group that corresponds to $P_{i_2}(i_2 < p-1)$. When $p = 2$, the head contains only positive substitutions. In this case the groups that correspond to P are distinct, since the one contains negative substitutions while the other does not.

By multiplying each substitution in the group (A) by t_2, we obtain a set of substitutions which with H generate the sets that transform according to p_2. Each of these transforms the head into itself, but t_2 is the only one that transforms $\{H, t_1\}$ into itself. For if we transform t_1 by the inverse of any other one, $s_is_j \ldots\ldots t_2$, say, we have

$$s_is_j \ldots\ldots t_2t_1t_2^{-1} s_is_j \ldots\ldots = s_is_j \ldots\ldots s_{i'}s_{j'} \ldots\ldots t_1^a,$$

where $t_2t_1t_2^{-1} = t_1^a$, and i', j' are certain ones of the subscripts $1, 2, \ldots\ldots, p$. There is an even number of s's in the part of this substitution that precedes t_1^a; further this part cannot be identity. Hence this substitution is not found in $\{H, t_1\}$, and, therefore, there is just one group that corresponds to P_{i_2} when $p > 2$.

4. THEOREM.— *When* $\dfrac{p-1}{i_2}$ *is even, there are two imprimitive groups of degree np that contain the head*

$$H \equiv G' \text{ pos } G'' \text{ pos } \ldots\ldots G^p \text{ pos}$$

and whose substitutions interchange the systems of intransitivity of H according to P_{i_2}. Where $\dfrac{p-1}{i_2}$ *is odd, there is just one such group.*

The largest group within which H is invariant without having its systems interchanged is $\{G', G'', \ldots\ldots, G^p\}$. There are then 2^p sets of substitutions that transform according to a given substitution of P_{i_2}. We know that there is just one distinct group that contains this head and corresponds to a cyclic substitution of order p. Hence it may be assumed that each group that contains H and that corresponds to P_{i_1} contains the substitution t_1.

The substitutions that permute according to p_2 may be found by multiplying H by the substitutions obtained by affixing t_2 to each substitution in the group

$$(s_1)(s_2)\ \ldots\ldots\ (s_p),$$

where s_i has the same meaning as in the preceding theorem. Of these generators t_2 and $s_1 s_2 \ldots\ldots s_p t_2$ are the only ones that transform $\{H, t_1\}$ into itself. The former has its $\frac{p-1}{i_2}$th power in H and generates with $\{H, t_1\}$ a group that corresponds to P_{i_2}. The latter has its $\frac{p-1}{i_2}$th power in the head only when $\frac{p-1}{i_2}$ is an even number. It transforms both H and $\{H, t_1\}$ into themselves. Hence, when $\frac{p-1}{i_2}$ is even, there are two groups that contain the given head and that correspond to P_{i_2}. The corresponding groups are distinct, since one contains negative substitutions while the other does not.

5. THEOREM.—*The number of imprimitive groups of degree np that contain the head*

$$H \equiv \{G' \text{ pos}, G'' \text{ pos}, \ldots\ldots, G^p \text{ pos}\}_{1, 1, \ldots\ldots, 1}$$

and whose substitutions interchange the systems of intransitivity of H according to P_{i_2} is as follows:

(a). *When $p = 2$, there are two groups.*

(b). *When $p = 3$ and $n = 3$, there are two groups if $i_2 = p - 1$, and three groups if $i_2 < p - 1$.*

(c). *When $p > 3$ and $n = 3$ or $p > 2$ and $n > 3$, there are two groups if $\frac{p-1}{i_2}$ is even and there is one group if $\frac{p-1}{i_2}$ is odd.*

In this case H is formed by writing after each substitution of G' pos the same substitutions in the other sets of elements.

(a). When $p=2$ and $n=3$, there are evidently two distinct groups. When $p=2$ and $n>3$, the only substitutions that permute according to p_1 and that also transform H into itself, may be obtained by multiplying H by the substitutions t_1 and $s_1s_2t_1$. Both of these have their squares in the head and they generate with H groups that are clearly distinct.

(b). When $p=3$ and $n=3$, the groups that are isomorphic to P_{p-1} are of order and degree 9. It follows that there are two such groups, since there are two distinct abstract groups of order p^2. They may be written $\{H, t_1\}$ and $\{H, a_1a_2a_3t_1\}$.

The substitutions that permute according to p_2 and that transform both H and $\{H, t_1\}$ into themselves may be obtained from the head by means of the substitutions

$$\begin{array}{ll} t_2, & s_1s_2s_3t_2, \\ S_1S_2^2t_2, & S_1S_2^2s_1s_2s_3t_2, \\ S_1^2S_2t_2, & S_1^2S_2s_1s_2s_3t_2, \end{array}$$

where $S_1=a_1a_2a_3$, $S_2=b_1b_2b_3$, etc. Each of these has its square in the head except the last two in the second column. Those in the first column clearly generate with $\{H, t_1\}$ conjugate groups. The groups $\{H, t_1, t_2\}$ and $\{H, t_1, s_1s_2s_3t_2\}$ are distinct since one contains only positive substitutions while the other contains negative substitutions.

The group $\{H, a_1a_2a_3t_1\}$ is a cyclic group of order 9. If a group that corresponds to P contains it self-conjugately, then that group is of order 18. There is just one such non-abelian group of this order,* and it can be represented in only one way as an imprimitive group of degree 9. Hence there is just one group with the head H that contains $\{H, a_1a_2a_3t_1\}$ self-conjugately and that corresponds to P.

(c). When $p>3$ and $n=3$, the groups that are isomorphic to P_{p-1} are of order and degree $p.3$. Since $p>3$ and the subgroup of order 3 is self-conjugate, it follows that there is just one group that contains H and that corresponds to P_{p-1}. It may be written $\{H, t_1\}$.

---

* Cole and Glover, American Journal of Mathematics, Vol. 15 (1893), p. 206.

The general substitution that permutes according to p_2 may be taken of the form

$$S_1^{\alpha_1} S_2^{\alpha_2} \ldots\ldots S_p^{\alpha_p} (s_1 s_2 \ldots\ldots s_p)^{\beta}\, t_2, \tag{A}$$

where $\alpha_1, \alpha_2, \ldots\ldots, \alpha_p = 0, 1, 2$ and $\beta = 0, 1$. If this substitution transforms $\{H, t_1\}$ into itself, then $S_1^{\alpha_1} S_2^{\alpha_2} \ldots\ldots S_p^{\alpha_p}$ must also do so. Now

$$S_1^{\alpha_1} S_2^{\alpha_2} \ldots\ldots S_p^{\alpha_p} t_1, \quad S_1^{-\alpha_1} S_2^{-\alpha_2} \ldots\ldots S_p^{-\alpha_p} = S_1^{\alpha_1 - \alpha_2} S_2^{\alpha_2 - \alpha_3} \ldots\ldots S_p^{\alpha_p - \alpha_1} t_1.$$

If this be in $\{H, t_1\}$, it must be of the form

$$(S_1 S_2 \ldots\ldots S_p)^{\alpha}\, t_1.$$

That is, we have the relations

$$\alpha_i - \alpha_1 \equiv -(i-1)\,\alpha \qquad (\text{mod } 3),$$

where $i = 1, 2, \ldots\ldots, p$ and $\alpha = 0, 1, 2$. Putting $i = p$, we see that

$$\alpha p \equiv 0 \qquad (\text{mod } 3).$$

Hence zero is the only permissible value of α and of the substitutions (A), we need consider only

$$t_2 \text{ and } s_1 s_2 \ldots\ldots s_p t_2,$$

The first of these has its $\frac{p-1}{i_2}$th power in the head and hence generates with $\{H, t_1\}$ a group that corresponds to P_{i_2}. The second has its $\frac{p-1}{i_2}$th power in the head only when $\frac{p-1}{i_2}$ is an even number.

Therefore, when $\frac{p-1}{i_2}$ is even, there are two groups that contain the given head and that correspond to P_{i_2}. They are distinct, since one contains only positive substitutions while the other contains only negative ones.

When $p > 2$ and $n > 3$, the substitutions that permute like p_1 and that transform H into itself, may be found by multiplying H by the substitutions

$$t_1 \text{ and } s_1 s_2 \ldots\ldots s_p t_1.$$

Of these only the first has its p^{th} power in the head, and hence there is just one group that contains the given head and is isomorphic to P_{p-1}. The remain-

ing part of the proof for this case is the same as the latter part of the preceding one.

6. The group $\{G', G'', \ldots, G^p\}$ may also be used as a head. It contains all the substitutions which transform it into itself without interchanging its systems of intransitivity. Hence it is contained as a head in just one imprimitive group whose substitutions permute its systems of intransitivity according to a given transitive group. The same remark applies to the head $\{G', G'', \ldots, G^p\}_{1, 1, \ldots, 1}$.*

7. The remaining theorems in this section apply to imprimitive groups of degree pq where p and q are prime numbers which may be the same or different primes.

Let G_1 denote the metacyclic group in the elements $a_1, a_2, \ldots, a_q$; G_2, the metacyclic group in the elements $b_1, b_2, \ldots, b_q$; $\ldots$; G_p, the same group in the elements $m_1, m_2, \ldots, m_q$; and let G_{i, i_1} denote that invariant subgroup of G_i whose index under G_i is i_1. The symbols P, P_{i_2}, p_1, p_2, t_1 and t_2 will be used as they were in the theorems just given. We shall assume further that the group G_1 is generated by the substitution $S_1 = a_1 a_2 a_3 \ldots a_q$ of order q, and a substitution S_1 of order $q-1$ in the $q-1$ elements $a_2, a_3, a_4, \ldots, a_q$. The symbols S_i and s_i will denote the same substitutions in the elements of the group G_i, where $i = 2, 3, \ldots, p$, as S_1 and s_1 do in the elements of G_1.

8. THEOREM.—*The number of imprimitive groups of degree pq that contain the head*

$$H \equiv \{G_{1, i_1}, G_{2, i_1}, \ldots, G_{p, i_1}\}$$

and whose substitutions interchange the systems of intransitivity of H according to P_{i_2}, is equal to the number of solutions of the congruences

$$\beta\left(\frac{p-1}{i_2}\right) \equiv h i_1 \qquad (\text{mod } q-1),$$

where β is restricted to the values 0, 1, 2, $\ldots$, $i-1$ and *h is any integer.*

---

* Miller, Quarterly Journal of Mathematics, Vol. 28 (1895), p. 195.

The largest group within which H is invariant without having its systems interchanged is $\{G_1, G_2, \ldots, G_p\}$. There are accordingly i_1^p sets of substitutions that transform according to each substitution of P_{i_2}.

Since the given head is the direct product of p transitive groups written in different sets of elements, we know that there is just one distinct group that contains this head and that corresponds to P_{p-1}. This may be taken as $\{H, t_1\}$ and we may assume that each group to be found contains this as a self-conjugate subgroup.

As $s_i^{i_1}$ is the lowest power of s_i besides s_i^0 that occurs in G_{i, t_1}, it follows that the i_1^p sets of substitutions that permute according to p_2 may be obtained by multiplying the head by the substitutions

$$s_1^{\alpha_1} s_2^{\alpha_2} \ldots s_p^{\alpha_p} t_2, \tag{A}$$

where $\alpha_1, \alpha_2, \ldots, \alpha_p = 0, 1, 2, \ldots,$ or $i_1 - 1$. For it is clear that these sets contain no common substitutions, and since each exponent may have i_1 different values, there are i_1^p of them. Each of the substitutions (A) that can be used must transform $\{H, t_1\}$ into itself. This will be true when $s_1^{\alpha_1} s_2^{\alpha_2} \ldots s_p^{\alpha_p}$ transforms t_1 into a substitution in $\{H, t_1\}$. The substitution

$$s_1^{\alpha_1} s_2^{\alpha_2} \ldots s_p^{\alpha_p} t_1 s_1^{-\alpha_1} s_2^{-\alpha_2} \ldots s_p^{-\alpha_p} = s_1^{\alpha_1 - \alpha_2} s_2^{\alpha_2 - \alpha_3} \ldots s_p^{\alpha_p - \alpha_1} t_1$$

will be found in $\{H, t_1\}$ only when what precedes t_1 is a substitution in H. Since the difference between any two different α's is less than i_1—the lowest exponent of s_i in G_{i, t_1} besides zero—it follows that we must have

$$\alpha_1 = \alpha_2 = \ldots = \alpha_p = \beta,$$

where $\beta = 0, 1, 2, \ldots,$ or $i_1 - 1$. Hence we need consider only the i_1 substitutions of the form

$$(s_1 s_2 \ldots s_p)^\beta t_2.$$

If any of these i_1 substitutions generates with $\{H, t_1\}$ a group that corresponds to P_{i_2} $(i_2 < p - 1)$, its $\frac{p-1}{i_2}$-th power must be in the head. This will be true only when the corresponding β satisfies one of the congruences

$$\beta\left(\frac{p-1}{i_2}\right) \equiv h i_1 \qquad (\text{mod } q - 1), \tag{1}$$

where h is any integer. Suppose that β_1 and β_2 are any two distinct values of

β, each of which satisfies one of these congruences. Each gives rise to a group that corresponds to P_{i_2} ($i_2 < p - 1$). Further, the resulting groups are distinct. If one could be transformed into the other by a substitution (s), then s would have to transform H into itself, since H is the only invariant intransitive subgroup of order $\left[\frac{q(q-1)}{i_1}\right]^p$ that is contained in either. It follows, therefore, that s must transform the division containing $(s_1 s_2 \ldots s_p)^{\beta_1} t_2$ into that containing $(s_1 s_2 \ldots s_p)^{\beta_2} t_2$, the divisions being formed with respect to $\{H, t_1\}$. This clearly cannot be done. Hence the number of imprimitive groups that correspond to P_{i_2} ($i_2 < p - 1$) is equal to the number of values of β (where $\beta = 0, 1, \ldots, i_1 - 1$) that satisfy the congruences (1).

9. THEOREM.—*The number of imprimitive groups of degree pq that contain the head*

$$H \equiv \{G_{1,i_1}, G_{2,i_1}, \ldots, G_{p,i_1}\}_{1,1,\ldots,1}$$

and whose substitutions interchange the systems of intransitivity of H according to P_{i_2} is as follows when $p \neq q$:

When $i_2 = p - 1$ there are two groups if i_1 is a multiple of p, but just one group if i_1 is not a multiple of p.

When $i_2 < p - 1$, the number of groups is equal to the number of solutions of the congruences

$$\beta\left(\frac{p-1}{i_2}\right) \equiv hi_1 \qquad (\mathrm{mod}\ q-1),$$

where h is any integer and β is restricted to the values $0, 1, 2, \ldots, i_1 - 1$.

The head is formed by writing after each substitution in G_{1,i_1} the same substitution in the other sets of letters.

I. Suppose that $i_1 < q - 1$.

In this case the largest group within which H is invariant without having its systems interchanged is $\{G_1, G_2, \ldots, G_p\}_{1,1,\ldots,1}$. This is of order $q(q-1)$ while H is of order $q(q-1)/i_1$. There are then i_1 sets of substitutions that transform according to any substitution in P_{i_2}. Since $(s_1 s_2 \ldots s_p)^{i_1}$ is the lowest power of $s_1 s_2 \ldots s_p$ that occurs in H, it is clear that the i_1 sets of substitu-

tions that transform according to p_1 may be obtained by multiplying the substitutions in the head by

$$(s_1 s_2 \ldots . s_p)^a t_1, \tag{A}$$

where $a = 0, 1, 2, \ldots, i_1 - 1$. The p^{th} power of each of these substitutions that generates with H a group corresponding to P_{p-1}, must be in H. This will be true only when a satisfies one of the congruences

$$ap \equiv hi_1 \pmod{q-1}, \tag{1}$$

where h is any integer. These congruences may be written in the form

$$ap = hi_1 + k(q-1),$$
$$= (h + kM)\, i_1,$$

where k is any integer and M equals $(q-1)/i_1$. Hence

$$a = \frac{h + kM}{p} i_1.$$

From this equation it follows that zero is the only value of a less than i_1 that satisfies the congruence (1) unless i_1 is a multiple of p. If, however,

$$i_1/p = m,$$

m being an integer, then a may have the values $0, m, 2m, \ldots, (p-1)\,m$. Hence when i_1 is a multiple of p, the substitutions (A) may be replaced by the substitutions

$$(s_1 s_2 \ldots . s_p)^{mx} t_1,$$

where $x = 0, 1, 2, \ldots, p-1$. Each of these substitutions generates with the head a group that corresponds to P_{p-1}, but it can be proved that only two of them are distinct. In the group that contains the substitution $(s_1 s_2 \ldots . s_p)^m t$ are found the substitutions $(s_1 s_2 \ldots . s_p)^{my} t_1^y$, where y may have any of the values 1, 2, , ..., $p-1$. If now p_2 be of order $p-1$, then a suitable power of the substitution t_2 that permutes according to p_2 will transform the head into itself and the substitution $(s_1 s_2 \ldots . s_p)^{mx} t_1$ into $(s_1 s_2 \ldots . s_p)^{mx} t_1^x$ if x is different from zero. Hence the $p-1$ groups $\{H, (s_1 s_2 \ldots . s_p)^{mx} t_1\}$, when x has the values $1, 2, \ldots, p-1$, are conjugate. The groups $\{H, t_1\}$ and $\{H, (s_1 s_2 \ldots . s_p)^m t_1\}$ are distinct abstract groups, since one contains an invariant operator of order p while the other does not. Hence it is proved that when i_1 is divisible by p, there are two groups containing the given head that

correspond to P_{p-1}, while when i_1 is not divisible by p, there is just one such group.

The i_1 sets of substitutions that transform according to p_2 may be obtained by multiplying the substitutions in the head by

$$(s_1 s_2 \ldots . s_p)^\beta t_2,$$

where β may take the values 0, 1, ..., $i_1 - 1$. Each of these transforms both the head and $\{H, t_1\}$ into themselves. The $\frac{p-1}{i_2}$th power of $(s_1 s_2 \ldots . s_p)^\beta t_2$ will be found in the head only when β satisfies one of the relations

$$\beta\left(\frac{p-1}{i_2}\right) \equiv h i_1 \qquad (\text{mod } q-1), \tag{2}$$

where h is any integer. Each value of β that satisfies one of these congruences gives then a substitution which generates with $\{H, t_1\}$ a group that corresponds to P_{t_2} $(i_2 < p-1)$. And by the argumeut used in the preceding theorem, it follows that the groups thus obtained are all distinct. Hence the number of groups that contain $\{H, t_1\}$ as an invariant subgroup and that correspond to P_{t_2} $(i_2 < p-1)$ is equal to the number of values of β that satisfy the congruences (2), β being restricted to the numbers 0, 1, ..., $i_1 - 1$.

If $\{H, (ss \ldots . s)^m t_1\}$ is contained as an invariant subgronp of a group that corresponds to P_{t_2}, then

$$(s_1 s_2 \ldots . s_p)^\beta t_2 (s_1 s_2 \ldots . s_p)^m t_1 t_2^{-1} (s_1 s_2 \ldots . s_p)^{-\beta} = (s_1 s_2 \ldots . s_p)^m t_1^\gamma$$

must be a substitution in $\{H, (s_1 s_2 \ldots . s_p)^m t_1\}$; γ is defined by the relation $t_2 t_1 t_2^{-1} = t_1^\gamma$. If this be true, it must occur in the division in which $[(s_1 s_2 \ldots . s_p)^m t_1]^\gamma$, or $(s_1 s_2 \ldots . s_p)^{m\gamma} t_1^\gamma$ is found. In this division $s_1 s_2 \ldots . s_p$ occurs to the powers $m\gamma + h i_1$. Hence there must be a relation of the form

$$m\gamma + h i_1 \equiv m \quad (\text{mod } q-1),$$

$$\therefore \quad m(\gamma - 1) = (kM - h)\, i_1, \text{ (where } q - 1 = M i_1),$$

$$\therefore \quad m = \frac{i_1}{p} = \frac{kM - h}{\gamma - 1}\, i_1,$$

$$\text{or} \quad \gamma - 1 = p\,(kM - h).$$

This equation however cannot exist, since γ is not congruent to unity modulus p. Hence there is no group that contains $\{H, (S_1 S_2 \ldots . S_p)^m t_1\}$ as an invariant subgroup and that corresponds to P_{t_2}, i_2 being different from $p - 1$.

II. Suppose that $i_1 = q - 1$.

In this case the largest group within which the head is invariant without having its systems interchanged is $\{G_1, G_2, \ldots, G_p\}_{q, q, \ldots, q}$. This latter group is formed by multiplying the corresponding divisions with respect to the self-conjugate subgroup of order q in the different sets of elements.

The groups that contain the given head and are isomorphic to P_{p-1} are of order and degree pq. We know, then, that when p is not a divisor of $q-1$, there is just one such imprimitive group, and that when p is a divisor of $q-1$, there are two such groups. These two groups may be taken as $\{H, t_1\}$ and $\{H, (ss \ldots s)^m t_1\}$, where $m = (q-1)/p$,

The most general substitution that permutes according to p_2 is of the form

$$S_1^{\alpha_1} S_2^{\alpha_2} \ldots S_p^{\alpha_p} (s_1 s_2 \ldots s_p)^\beta t_2,$$

where $\alpha_1, \alpha_2, \ldots, \alpha_p = 0, 1, \ldots, q-1$ and $\beta = 0, 1, \ldots, q-2$. If this substitution transforms $\{H, t_1\}$ into itself, then $S_1^{\alpha_1} S_2^{\alpha_2} \ldots S_p^{\alpha_p}$ must also do so. Now

$$S_1^{\alpha_1} S_2^{\alpha_2} \ldots S_p^{\alpha_p} t_1 S_1^{-\alpha_1} S_2^{-\alpha_2} \ldots S_p^{-\alpha_p} = S_1^{\alpha_1 - \alpha_2} S_2^{\alpha_2 - \alpha_3} \ldots S_p^{\alpha_p - \alpha_1} t_1.$$

If this be in $\{H, t_1\}$, it must be of the form

$$(S_1 S_2 \ldots S_p)^\alpha t_1.$$

That is, we must have the relations

$$\alpha_i - \alpha_1 \equiv -(i-1)\alpha \qquad (\text{mod } q),$$

where $i = 1, 2, \ldots, p$ and α has one of the values $0, 1, \ldots, q-1$. Such can be the case only when

$$\alpha p \equiv 0 \qquad (\text{mod } q).$$

Zero is the only value of α less than q that satisfies this congruence, and hence we must have $\alpha_1 = \alpha_2 = \ldots = \alpha_p$. The substitutions that permute according to p_2 which are to be considered, may therefore be obtained by multiplying the substitutions of the head by the substitutions

$$(s_1 s_2 \ldots s_p)^\beta t_2,$$

where $\beta = 0, 1, 2, \ldots, q-1$. If the $\frac{p-1}{i_2}$th power of any of these be in the head, the corresponding β must satisfy the congruence

$$\beta\left(\frac{p-1}{i_2}\right) \equiv 0 \qquad (\text{mod } q-1).$$

To each such β there corresponds a distinct group, containing $\{H, t_1\}$ self-conjugately; hence formula (2) is true for all values of i_1.

It remains to find if $\{H, (s_1 s_2 \ldots s_p)^m t_1\}$ is contained as an invariant subgroup in a group that corresponds to P_{i_2}, where i_2 is less than $p-1$. If we transform $(s_1 s_2 \ldots s_p)^m t_1$ by the inverse of the general substitution

$$s_1^{a_1} s_2^{a_2} \ldots s_p^{a_p} (s_1 s_2 \ldots s_p)^\beta t_2$$

we get a substitution of the form

$$s_1^{a_1'} s_2^{a_2'} \ldots s_p^{a_p'} (s_1 s_2 \ldots s_p)^m t_1^\gamma.$$

This could not occur in $\{H, (s_1 s_2 \ldots s_p)^m t_1\}$; for it would have to be found in the division in which $(s_1 s_2 \ldots s_p)^{m\gamma} t_1^\gamma$ occurs and we would then have the relation

$$m\gamma \equiv m \qquad (\text{mod } q-1),$$

or

$$m(\gamma - 1) = k(q-1).$$

or

$$\gamma - 1 = k\frac{q-1}{m} = kp.$$

This cannot be true since γ is not congruent to unity modulus p. Hence the given group is not contained self-conjugately in a group that corresponds to P_{i_2}, where $i_2 < p-1$.

When $p = q$ and $i_1 < p-1$, the above argument shows that there is just one group containing H that corresponds to P_{p-1}; and that when $i_2 < p-1$, the number that corresponds to P_{i_2} is not greater than the number of solutions of the congruences

$$\beta\left(\frac{p-1}{i_2}\right) \equiv hi_1 \qquad (\text{mod } p-1),$$

where β is restricted to the values $0, 1, 2, \ldots, i_1 - 1$ and h is any integer.

When $p = q$ and $i_1 = p-1$, the groups that correspond to P_{i_2} are easily determined by considering the holomorphs of the two regular groups of order p^2. In the holomorph of the cyclic group of order p^2 there is clearly just one group that contains the given head and that corresponds to P_{i_2}.

10. THEOREM.—*When* $i_2 = p-1$ *and* $\frac{q-1}{i_1}$ *is not a multiple of* p, *there is one imprimitive group of degree* pq *that contains the head*

$$H \equiv \{G_{1,i_1}, G_{2,i_1}, \ldots, G_{p,i_1}\}_{q,q,\ldots,q},$$

whose substitutions interchange the systems of intransitivity of H according to P_{i_2}; when $i_2 = p - 1$ and $\frac{q-1}{i_1}$ is a multiple of p, there are two such groups.

When $i_2 < p - 1$, the number of groups is equal to the number of solutions of the congruences

$$\beta\left(\frac{p-1}{i_2}\right) \equiv hi_1 \qquad (\text{mod } q-1),$$

where h is any integer and β is restricted to the values $0, 1, 2, \ldots, i_1 - 1$.

The given head in this case is formed by taking the product of corresponding divisions with respect to the invariant subgroup q of each of the transitive constituents. The largest group within which H is invariant without having its systems interchanged is $\{G_1, G_2, \ldots, G_p\}$. Hence we may take

$$s_1^{\alpha_1} s_2^{\alpha_2} \ldots s_p^{\alpha} t_1,$$

$\alpha_1, \alpha_2, \ldots, \alpha_p$ being integers, as the general substitution that transforms according to p_1. This substitution transforms the head into itself and with H generates a group that corresponds to P_{p-1}, in case its p^{th} power is found in the head. This will be true if the α's satisfy one of the relations

$$\alpha_1 + \alpha_2 + \ldots + \alpha_p \equiv hi, \qquad (\text{mod } q-1), \tag{1}$$

h being any integer.

We first show that the groups that correspond to different solutions of any given one of these $\frac{q-1}{i_1}$ congruences—this being the number of distinct relations (1)—are conjugate. For, let h_1 be any value of h, and let $\alpha_1, \alpha_2, \ldots, \alpha_p$ and $\alpha_1', \alpha_2', \ldots, \alpha_p'$ be two distinct solutions of the corresponding congruence. Then

$$\begin{aligned} &s_1^{\beta_1} s_2^{\beta_2} \ldots s_p^{\beta_p} s_1^{\alpha_1} s_2^{\alpha_2} \ldots s_p^{\alpha_p} t_1 s_1^{-\beta_1} s_2^{-\beta_2} \ldots s_p^{-\beta_p} \\ &\qquad = s_1^{\beta_1 - \beta_2 + \alpha_1} s_2^{\beta_2 - \beta_3 + \alpha_2} \ldots s_p^{\beta_p - \beta_1 + \alpha_p} t_1 = s_1^{\alpha_1'} s_2^{\alpha_2'} \ldots s_p^{\alpha_p'} t_1, \end{aligned}$$

when $\beta_i = \beta_1 + (\alpha_1 + \alpha_2 + \ldots + \alpha_{i-1}) - (\alpha_1' + \alpha_2' + \ldots + \alpha_{i-1}')$ where $i = 2, 3, \ldots, p$. Also $s_1^{\beta_1} s_2^{\beta_2} \ldots s_p^{\beta_p}$ transforms the head into itself. Hence there cannot be more than $\frac{q-1}{i_1}$ distinct groups that correspond to P_{p-1}—one to each of the above congruences.

The substitutions in the following table give a set of $q-1$ generators—one corresponding to each congruence—which, with the given head, generate one set of $\frac{q-1}{i_1}$ groups isomorphic to P_{p-1}:

$$\begin{array}{cccc} t_1, & s_1^{i_1}\,t_1, & & s_1^{(p-1)i_1}\,t_1, \\ (s_1s_2\,\ldots\,s_p)^{i_1}t_1\,, & s_1^{i_1}(s_1s_2\,\ldots\,s_p)^{i_1}\,t_1, & \ldots\,, & s_1^{(p-1)i_1}(s_1s_2\,\ldots\,s_p)^{i_1}\,t_1\,, \\ (s_1s_2\,\ldots\,s_p)^{2i_1}t_1, & s_1^{i_1}(s_1s_2\,\ldots\,s_p)^{2i_1}\,t_1, & \ldots\,, & s_1^{(p-1)i_1}(s_1s_2\,\ldots\,s_p)^{2i_1}\,t_1, \\ \vdots & \vdots & \ldots & \vdots \end{array}$$

the table being continued until $\frac{q-1}{i_1}$ substitutions are contained in it.

In the first place it is evident that the groups that correspond to the substitutions in the i^{th} column where $i=1, 2, \ldots, p$, are identical. Hence we need consider only those groups that correspond to the substitutions in the first row. In the group $\{H, s_1^{i_1}t_1\}$ are found the substitutions

$$(s_1 s_p s_{p-1}\,\ldots\,s_{p-x+2})^{i_1}\,t_1,$$

where $x=2, 3, \ldots, p-1$. If p_2 be of order $p-1$, then a certain power of the substitution t_2 that transforms according to p_2 will transform t_1^x into t_1 and the group $\{H, s_1^{i_1}t_1\}$ into a group that is conjugate to $\{H, s_1^{xi_1}t_1\}$. Hence the groups $\{H, s_1^{ri_1}t_1\}$, where $r=1, 2, \ldots, p-1$ are conjugate. We consider then the two groups $\{H, t_1\}$ and $\{H, s_1^{i_1}t_1\}$. The latter contains in the division in which $s_1^{i_1}t_1$ occurs the substitutions

$$S_1^{\alpha_1'}S_2^{\alpha_2'}\,\ldots\,S_p^{\alpha_p'}\,S_1^{hi_1+i_1}(s_2s_3\,\ldots\,s_p)^{hi_1}\,t_1,$$

where $\alpha_1', \alpha_2', \ldots, \alpha_p' = 0, 1, \ldots,$ or $q-1$ and h is any integer. If the p^{th} power of any of these be identity, then

$$\begin{aligned} &(hp+1)\,i_1 \equiv 0 \qquad (\mathrm{mod}\ q-1), \\ \text{or}\qquad &(hp+1)\,i_1 = k(q-1), \\ \text{or}\qquad &kM - hp \;= 1, \end{aligned} \tag{2}$$

if $M=(q-1)/i_1$. When M is not a multiple of p, this equation has a solution. In this case there is a substitution of order p in the division in question. The corresponding exponents of the s's then satisfy the first congruence of (1), and the group is conjugate to $\{H, t_1\}$. When, however, $\frac{q-1}{i_1}=mp$, where m is an

integer, then (2) becomes

$$(km - h)\,p = 1\,.$$

This has no solution. Hence when $(q-1)/i_1$ is not a multiple of p, there is just one group containing the given head that corresponds to P_{p-1}; but when $(q-1)/i_1$ is a multiple of p, there are two such groups.

The general form of the generating substitutions that transform according to p_2 is

$$s_1^{\alpha_1} s_2^{\alpha_2} \ldots\ldots s_p^{\alpha_p}\, t_2\,.$$

If any of these transform $\{H, t_1\}$ into itself, then $s_1^{\alpha_1} s_2^{\alpha_2} \ldots\ldots s_p^{\alpha_p}$ must do so. That is,

$$s_1^{\alpha_1} s_2^{\alpha_2} \ldots\ldots s_p^{\alpha_p}\, t_1\, s_1^{-\alpha_1}\, s_2^{-\alpha_2} \ldots\ldots s_p^{-\alpha_p} = s_1^{\alpha_1-\alpha_2} s_2^{\alpha_2-\alpha_3} \ldots\ldots s_p^{\alpha_p-\alpha_1}\, t_1$$

must be of the form

$$(s_1 s_2 \ldots\ldots s_p)^{\alpha}\, t_1,$$

where α is some multiple of i_1. That is, we have the relations

$$\alpha_i \equiv \alpha_1 - (i-1) \qquad (\text{mod } q-1).$$

Putting $i = p$, it is seen that

$$\alpha p \equiv 0 \qquad (\text{mod } q-1),$$

i. e.,

$$\alpha = k\,\frac{q-1}{p}\,.$$

Hence, as the values of α to be considered are multiples of i_1 that are less than $q-1$, it follows that $q-1$ must be a multiple of pi_1 unless $\alpha = 0$. In the latter case, $\alpha_1 = \alpha_2 = \ldots\ldots = \alpha_p$. That is, when $(q-1)/i_1$ is not a multiple of p, the substitutions that permute according to p which we have to consider may be obtained by multiplying the head by the substitutions

$$(s_1 s_2 \ldots\ldots s_p)^{\beta}\, t_2,$$

where $\beta = 0, 1, 2, \ldots\ldots i_1 - 1$. When, however, $(q-1)/i_1 = mp$, we must multiply the head by

$$s_1^{\alpha_1}\, s_2^{\alpha_1-\alpha}\, s_3^{\alpha_1-2\alpha} \ldots\ldots s_p^{\alpha_1-(p-1)\alpha}\, t_2,$$

where $\alpha = 0, mi_1, 2mi_1, \ldots\ldots, (p-1)\,mi_1$. These may be written in the form

$$s_2^{(p-1)\alpha} s_3^{(p-2)\alpha} \ldots\ldots s_p^{\alpha}\, (s_1 s_2 \ldots\ldots s_p)^{\alpha_1}\, t_2.$$

If α_1' is a value of α_1 for which the $(p-1)/i_2^{\text{th}}$ power of this substitution is in the head, then there cannot be more than p groups that correspond to this value of α_1. We prove that there is just one—i. e., that the groups that correspond to the substitutions

$$s_2^{(p-1)\alpha} s_3^{(p-2)\alpha} \ldots\ldots s_p^{\alpha} (s_1 s_2 \ldots\ldots s_p)^{\alpha_1} t_2$$

are conjugate. For, transform the substitution $(s_1 s_2 \ldots\ldots s_p)^{\alpha_1'} t_2$ by the inverse of $s_2^{(p-1)\alpha} s_3^{(p-2)\alpha} \ldots\ldots s_p^{\alpha}$. This latter transforms $\{H, t_1\}$ into itself. Suppose that t_2^{-1} transforms S_x into S_2. Then the transform in question is of the form

$$s_2^{(x-2)\alpha} \ldots\ldots (s_1 s_2 \ldots\ldots s_p)^{\alpha_1'} t_2.$$

When α takes the values $0, mi_1, \ldots\ldots, (p-1)\, mi_1$, we get p different substitutions in this way. For, let imi_1 and jmi_1 be any two distinct values of α. If these gave rise to the same substitution, then we would have

$$(x-2)\, imi_1 \equiv (x-2) jmi_1 \pmod{q-1},$$

or

$$(x-2)(i-j)\, mi_1 = k(q-1) = kmpi_1,$$

or

$$(x-2)(i-j) = kp.$$

$$\therefore \quad x-2 \equiv 0 \pmod{p},$$

$$x \equiv 2 \pmod{p}.$$

This, however, is not true. Hence, in any case, the substitutions that transform according to p_2 may be found by multiplying H by the substitutions

$$(s_1 s_2 \ldots\ldots s_p)_1^{\beta} t_2,$$

where $\beta = 0, 1, \ldots\ldots, i_1 - 1$. As above (§8), we prove that to each value of β that satisfies the congruences

$$\beta\left(\frac{p-1}{i_2}\right) \equiv hi_1 \pmod{q-1},$$

there is a distinct group that contains $\{H, t_1\}$ as an invariant subgroup.

It remains to consider what (if any) groups contain $\{H, S_1^{i_1} t_1\}$ as an invariant subgroup which corresponds to P_{i_2}. The general substitution to be considered is, as before,

$$s_1^{\alpha_1} s_2^{\alpha_2} \ldots\ldots s_p^{\alpha_p}\ t_2.$$

Transforming $s_1^{i_1} t_1$ by this, we get

$$t_2^{-1} s_1^{-\alpha_1} \ldots\ldots s_p^{-\alpha_p} s_1^{i_1} t_1 s_1^{\alpha_1} \ldots\ldots s_p^{\alpha_p} t_2 = t_2^{-1} s_1^{\alpha_2 - \alpha_1 + i_1} s_2^{\alpha_3 - \alpha_2} \ldots\ldots s_p^{\alpha_1 - \alpha_p} t_1 t_2$$
$$= s_1^{\alpha_2 - \alpha_1 + i_1} s_{i_2}^{\alpha_3 - \alpha_2} s_{i_3}^{\alpha_4 - \alpha_3} \ldots\ldots s_{i_p}^{\alpha_1 - \alpha} t_1^{\gamma'}, \quad (\mathrm{A}_1)$$

where the subscripts $i_2, i_3, \ldots . i_p$ denote the numbers $2, 3, \ldots ., p$ in some order and where γ' is defined by $t_2^{-1} t_1 t_2 = t_1^{\gamma'}$. If this be a substitution in $\{H, s_1^{i_1} t_1\}$, it must occur in the division in which $(s_1^{i_1} t_1)^{\gamma'}$ or $(s_1 s_p \ldots . s_{p-\gamma'+2})^{i_1} t_1^{\gamma'}$ is found. In this division we have the substitutions

$$(s_1 s_2 \ldots . s_p)^{hi_1} (s_1 s_p \ldots . s_{p-\gamma'+2})^{i_1} t_1^{\gamma'}. \qquad (\mathrm{A}_2)$$

If (A_1) be identical with any of these, then the p^{th} power of each must give rise to the same substitution. Now the p^{th} power of (A_1) is $(s_1 s_2 \ldots . s_p)^{i_1}$, while that of (A_2) is $(s_1 s_2 \ldots . s_p)^{(hp+\gamma')i_1}$. Hence we must have the relation

$$(hp + \gamma') i_1 \equiv i_1 \qquad (\mathrm{mod}\ q - 1),$$

or

$$(hp + \gamma') i_1 = (1 + kmp) i_1, \qquad \left\{\text{since } \frac{q-1}{i_1} = mp\right\},$$

or

$$\gamma' = 1 + (km - h) p.$$

This, however, cannot be true, since γ' is not congruent to unity modulus p. Hence there is no group that contains $\{H, s_1^{i_1} t_1\}$ as an invariant subgroup and that corresponds to P_{i_2}, i_2 being different from $p - 1$.

11. Let H_{i_1} denote that invariant subgroup of

$$(S_1 S_2^{-1})(S_2 S_3^{-1}) \ldots . (S_{p-1} S_p^{-1})(s_1 s_2 \ldots . s_p)$$

whose index under G is i_1, p being an odd prime.

THEOREM.—*The number of imprimitive groups of degree pq that contain the head*

$$H_{i_1}$$

and whose substitutions interchange the systems of intransitivity of H_{i_1} according to P_{i_2} is as follows:

(a) *When $i_2 = p - 1$ and $p = q$ there are two groups if $i_1 = q - 1$ and one group if $i_1 < q - 1$.*

(b) *When $i_2 = p - 1$ and $p \neq q$ there is one group if i_1 is not a multiple of p and two groups if i_1 is a multiple of p.*

(c) *When $i_2 < p - 1$, $p \neq q$, and $i_1 = q - 1$ the number of groups is equal to the number of solutions of the congruences*

$$\beta \left(\frac{p-1}{i}\right) \equiv hi_1 \qquad (\mathrm{mod}\ q - 1), \qquad (1)$$

where h is any integer and $\beta = 0, 1, \ldots, i_1 - 1$ in case $\frac{p-1}{i_2}$ is not a multiple of q and one greater than this number in case $\frac{p-1}{i_2}$ is a multiple of q; when $i_2 < p - 1$, $p \neq q$, $i_1 < q - 1$ the number is given by (1).

(d) *When $i_2 < p - 1$ and $p = q$ the number is one greater than that given by the congruences* (1).

Suppose $i_1 = q - 1$.

In this case the largest group within which the given head is invariant without having its systems interchanged is $(S_1) \ldots (S_p)(s_1 s_2 \ldots s_p)$. This is of order $q^p(q-1)$, while H_{i_1} is of order q^{p-1}. There are then $q(q-1)$ sets of substitutions that transform according to any substitution in P_{i_2}. Now, H_{q-1} contains the substitutions

$$(S_1 S_2 \ldots S_{p-1})^a S_p^{a - pa},$$

where a is any integer. This substitution will be of the form $(S_1 S_2 \ldots S_p)^a$ when

$$ap \equiv 0 \qquad (\text{mod } q).$$

It follows that when p is different from q, there is no substitution of the form $(S_1 S_2 \ldots S_p)^a$ in H_{q-1}. In this case the substitutions that permute according to p_1 may be obtained by forming the products of the head and the following substitutions:

$$\begin{array}{llll}
t_1, & s_1 s_2 \ldots s_p t_1, & \ldots & (s_1 s_2 \ldots s_p)^{q-2} t_1 \\
(S_1 \ldots S_p) t_1, & (S_1 \ldots S_p) s_1 s_2 \ldots s_p t_1, & \ldots & (S_1 \ldots S_p)(s_1 s_2 \ldots s_p)^{q-2} t_1 \\
(S_1 \ldots S_p)^2 t_1, & (S_1 \ldots S_p)^2 s_1 s_2 \ldots s_p t_1, & \ldots & (S_1 \ldots S_p)^2 (s_1 s_2 \ldots s_p)^{q-2} t_1 \\
\vdots & \vdots & \ldots & \vdots \\
(S_1 \ldots S_p)^{q-1} t_1, & (S_1 \ldots S_p)^{q-1} s_1 s_2 \ldots s_p t_1, & \ldots & \\
 & & & (S_1 \ldots S_p)^{q-1} (s_1 s_2 \ldots s_p)^{q-2} t_\gamma
\end{array}$$

Of the substitutions in the first column t_1 is the only one whose p^{th} power is in the head. If the p^{th} power of any other one in the first row is in the head then this is true of all the substitutions in the corresponding column. But the resulting groups are conjugate, as is seen by transforming the one containing $(s_1 s_2 \ldots s_p)^\beta t_1$ by $(S_1 S_2 \ldots S_p)^a$ where β is the exponent of $s_1 s_2 \ldots s_p$ in the column in question and $a = 1, 2, \ldots, q-1$. We need consider then only the

substitutions in the first row. The p^{th} power of $(s_1s_2 \ldots\ldots s_p)^a t_1$ will be in the head if

$$ap \equiv 0 \pmod{q-1}.$$

When p is prime to $q-1$, zero is the only value that a may take and in this case there is just one group. When, however, $(q-1)/p$ equals an integer, m, then $a = 0, m, 2m, \ldots\ldots, (p-1)m$. But as above (§9) the groups that correspond to the values $m, 2m, \ldots\ldots, (p-1)m$ are conjugate and hence in this case there are two distinct groups that contain the given head and that correspond to P_{p-1}.

When p equals q the head contains the substitutions $(S_1S_2 \ldots\ldots S_p)^a$ where $a = 1, 2, \ldots\ldots, q-1$. The substitutions that permute according to p_1 may now be found by multiplying the head by the set of substitutions obtained by replacing $(S_1S_2 \ldots\ldots S_p)^a$ by S_1^a in the preceding table. Of these only those in the first column have their p^{th} power in the head. That is, we need consider only those of the form

$$S_1^a\, t_1$$

where $a = 0, 1, \ldots\ldots, p-1$. If $\{H, S_1\, t_1\}$ is transformed by $(s_1s_2 \ldots\ldots s_p)^\beta$ where $\beta = 0, 1, \ldots\ldots, p-2$, it is seen that the groups $\{H, S_1^x\, t_1\}$ where $x = 1, 2, \ldots\ldots, p-1$ are conjugate. The groups $\{H, t_1\}$ and $\{H, S_1\, t_1\}$ are distinct, since the former contains only substitutions of order p in the division in which t_1 occurs while the latter contains substitutions of order p^2 in this division.

When p is not equal to q, the substitutions that transform according to p_2 can be found by multiplying the head by the substitutions that result when t_1 is replaced by t_2 in the first of the above tables. If any substitution in the first column besides t_1 has its $(p-1)/i_2^{\text{th}}$ power in the head then $\frac{p-1}{i_2}$ must be a multiple of q. The groups $\{H, t_1, (S_1S_2 \ldots\ldots S_p)^x\, t_2\}$, where $x = 1, 2, \ldots\ldots, q-1$ are conjugate as is seen by transforming one of them by $(s_1s_2 \ldots\ldots s_p)^\beta$ where $\beta = 1, 2, \ldots\ldots, q-2$. But the groups $\{H, t_1, t_2\}$ and $\{H, t_1, (S_1S_2 \ldots\ldots S_p)\, t_2\}$ are clearly distinct. If any other substitution in the first row, besides t_2, has its $\frac{p-1}{i_2}$th power in the head, then all of those in the column to which it belongs also satisfy this condition. But the corresponding groups are conjugate, as is seen

on transforming one of them by $(S_1 S_2 \ldots . S_p)^{\alpha}$ where $\alpha = 1, 2, \ldots, q-1$. We need then to consider only substitutions of the form

$$(s_1 s_2 \ldots . s_p)^{\beta} t_2$$

where $\beta = 0, 1, \ldots, q-2$. As before, it follows that the number of distinct groups is equal to the number of values of β that satisfy the congruences

$$\beta \left(\frac{p-1}{i_2}\right) \equiv 0 \qquad (\text{mod } q-1).$$

If $\{H_{q-1}, (s_1 s_2 \ldots . s_p)^m t_1\}$ is contained as an invariant subgroup in a group that corresponds to P_{i_2} $(i_2 < p-1)$ then

$$t_2^{-1} (s_1 s_2 \ldots . s_p)^{-\beta} (S_1 S_2 \ldots . S_p)^{-\alpha} (s_1 s_2 \ldots . s_p)^m t_1 (S_1 S_2 \ldots . S_p)^{\alpha} (s_1 s_2 \ldots . s_p)^{\beta} t_2$$

or

$$(S_1 S_2 \ldots . S_p)^{\alpha'} \quad (s_1 s_2 \ldots . s_p)^m t_1^{\gamma_1}$$

must be a substitution of this group. This can be true only when it is identical with the substitution $(s_1 s_2 \ldots . s_p)^{m\gamma_1} t_1^{\gamma_1}$ — that is, when

$$m\gamma_1 \equiv m \qquad (\text{mod } q-1)$$

or

$$\gamma_1 \equiv 1 \qquad (\text{mod } p).$$

This equation, however, is not true, and hence there is no group of the kind in question.

When p equals q, we may replace t_1 by t_2 in the second of the above tables to obtain a set of substitutions which with H_{p-1} generate the substitutions that permute according to p_2. Those in the first column are of the form

$$S_1^{\alpha} t_2$$

where $\alpha = 0, 1, \ldots, p-1$. The $\frac{p-1}{i_2}$th power of this is in the head when

$$\alpha \left(\frac{p-1}{i_2}\right) \equiv 0 \qquad (\text{mod } p)$$

or

$$\alpha = \frac{kpi_2}{p-1}.$$

It follows that zero is the only permissible value of α. If any substitution in the first row has its $\frac{p-1}{i_2}$th power in the head, then the corresponding β must satisfy the relation

$$\beta \left(\frac{p-1}{i_2}\right) \equiv 0 \qquad (\text{mod } p-1), \tag{1}$$

where $\beta=0, 1, 2, \ldots, p-2$. If β_1 be any solution of this congruence besides zero, then it is clear that all the substitutions in the same column with $(s_1s_2\ldots s_p)^{\beta_1}t_2$ have their $\frac{p-1}{i_2}$th power in the head. Now all of these substitutions that have their $\frac{p-1}{i_2}$th power in the head also transform $\{H_{p-1}, t_1\}$ into itself. But those which belong to the same column give rise to conjugate groups as is seen by transforming by S_1^x where $x=1, 2, \ldots, p-1$. Hence the number of distinct groups that contain $\{H_{p-1}, t_1\}$ as an invariant subgroup is equal to the number of solutions of the congruence (1).

If $(s_1s_2\ldots s_p)^{\beta_1}t_2$ transforms $\{H_{p-1}S_1\,t_1\}$ into itself, so also will $S_1^{\alpha_1}(s_1s_2\ldots s_p)^{\beta_1}t_2$. We need consider then only those substitutions in the first row whose exponents satisfy (1). Now if β_1 be such a value of the exponent, then

$$t_2^{-1}(s_1s_2\ldots s_p)^{-\beta_1}S_1t_1(s_1s_2\ldots s_p)^{\beta_1}t_2=s_1^{-\beta_1}S_1s_1^{\beta_1}t_1^{\gamma_1}=S_1^{\alpha'}t_1^{\gamma_1},$$

where $t_2^{-1}t_1t_2=t_1^{\gamma_1}$ and $s_1^{-\beta_1}S_1s_1^{\beta}=S_1^{\alpha'}$. This will evidently be a substitution in $\{H_{p-1}, S_1\,t_1\}$ only when $\alpha'=\gamma_1$. Hence, there is just one substitution in the first row that transforms the given group into itself—the corresponding value of β being i_2. All the substitutions in the corresponding column give rise to conjugate groups, as may be seen by transforming $\{H, S_1t_1, (s_1s_2\ldots s_p)^{i_2}t_2\}$ by S_1^{α}, where $\alpha=1, 2, \ldots, p-1$. Hence, there is just one group that contains $\{H, S_1t_1\}$ and that corresponds to P_{i_2}.

(2). When $i_1<q-1$.

In this case, the largest group within which the given head is invariant without having its systems interchanged is

$$(S_1S_2^{-1})(S_2S_3^{-1})\ldots(S_{p-1}S_p^{-1})(s_1s_2\ldots s_p).$$

There are then i_1 sets of substitutions that transform according to any substitution in P_{i_2}. Those that transform according to P_{p-1} may be obtained by multiplying the head by the substitutions

$$(s_1s_2\ldots s_p)^{\alpha}t_1,$$

where $\alpha=0, 1, \ldots, i_1-1$. If the p^{th} power of any of these be in the head,

then the corresponding α must satisfy the relation

$$\alpha p \equiv h i_1 \qquad (\text{mod } q-1),$$

where h is as usual. That is,

$$\alpha p = (h + kM)\, i_1 \qquad \left\{\frac{q-1}{i_1} = M\right\}.$$

When i_1 is not a multiple of p, zero is the only value of α that can be used; when $i_1 = mp$ (where m is an integer), then $\alpha = 0, m, 2m, \ldots, (p-1)\,m$. Hence, as before, when p is prime to i_1, there is just one group that corresponds to P_{p-1}, and when $i_1 = mp$, there are two such groups.

The substitutions that transform according to p_2 result when the head is multiplied by the substitutions

$$(s_1 s_2 \ldots . s_p)^{\beta}\, t_2,$$

where $\beta = 0, 1, \ldots, i_1 - 1$. Each of these transforms both the head and $\{H_{i_1}, t_1\}$ into themselves. The number of groups that contain $\{H_{i_1}, t_1\}$ self-conjugately and that correspond to P_{i_2} is then equal to the number of solutions of the congruences

$$\beta\left(\frac{p-1}{i_2}\right) \equiv h i_1 \qquad (\text{mod } q-1),$$

where h is as usual.

By the reasoning used above, it follows that there is no group isomorphic to P_{i_2} that contains $\{H_{i_1}, (s_1 s_2 \ldots . s_p)^m t_1\}$ as an invariant subgroup, where $i_2 < p-1$.

12. Consider the head which may be written in the form

$$H \equiv (s_1 s_2^{-1})(s_2 s_3^{-1})(s_3 s_4^{-1}) \ldots . (s_{p-1} s_p^{-1}).$$

To form the group which this represents, we first establish the $q:q$ isomorphism between G_1 and G_2 in which the division containing s_2^{-1} in G_2 corresponds to that containing s_1 in G_1. Denote this group by h_1. Then establish the $q^2(q-1):q$ isomorphism between $\{h_1, s_2\}$ and G_3 in which the division containing s_3^{-1} in G_3 corresponds to that containing s_2 in the group $\{h_1, s_2\}$—the divisions in the latter group being formed with respect to h_1. Denote the resulting group by h_2 and establish a similar isomorphism between $\{h_2, s_3\}$ and G_4; that is, make the division containing s_4^{-1} in G_4 correspond to the division containing

s_3 in $\{h_2, s_3\}$—the divisions being formed with respect to h_2 in the latter group. Continue this process until all the p groups G_i have been used. The resulting group evidently permits a cyclic interchange of the systems, and hence may be used as a head. It further permits the interchange of the systems required by p_2, and we now consider the groups that contain this head and that correspond to P_{i_2}.

THEOREM.—*When $i_2 = p - 1$ and $q - 1$ is a multiple of p, there are two groups that contain the head H, whose substitutions interchange the systems of intransitivity of H according to P_{i_2}; when $i_2 = p - 1$ and $q - 1$ is prime to p, there is just one such group.*

When $i_2 < p - 1$, the number of groups is equal to the number of solutions of the congruence

$$\beta\left(\frac{p-1}{i_2}\right) \equiv 0 \qquad (\text{mod } q-1),$$

where $\beta = 0, 1, 2, \ldots, q-2$.

The largest group within which the given head is invariant without having its systems interchanged is $\{G_1, G_2, \ldots G_p\}$. This is of order $q^p(q-1)^p$ while the head is of order $q^p(q-1)^{p-1}$. Hence there are $q-1$ sets of substitutions that permute according to any substitution in P_{i_2}. Those that transform according to p_1 may be found by multiplying the head by the substitutions

$$s_1^{\alpha} t_1, \tag{A}$$

where $\alpha = 0, 1, \ldots, q-2$. Each of these transforms the head into itself The p^{th} power of (A) will be in the head if α satisfies the congruence

$$\alpha p \equiv 0 \qquad (\text{mod } q-1). \tag{1}$$

For we find in the head the substitutions

$$s_1^{\alpha} s_2^{-\alpha}; \quad s_2^{2\alpha} s_3^{-2\alpha}; \quad s_3^{3\alpha} s_4^{-3\alpha}; \ldots ; s_{p-1}^{(p-1)\alpha} s_p^{-(p-1)\alpha}.$$

The product of these is $(s_1 s_2 \ldots s_{p-1})^{\alpha} s_p^{-(p-1)\alpha}$ and this will be identical with $(s_1 s_2 \ldots s_p)^{\alpha}$ only when

$$-(p-1)\alpha \equiv \alpha \qquad (\text{mod } q-1)$$

or

$$\alpha p \equiv 0 \qquad (\text{mod } q-1).$$

When p is not a divisor of $q-1$, zero is the only value of α less than $q-1$ that satisfies the congruence (1) and so in this case there is just one group containing the given head that corresponds to P_{p-1}. When, however, $(q-1)/p$ equals an

integer m, then $\alpha = 0,\ m,\ 2\,m, \ldots\ldots (p-1)m$ are solutions of (1). The substitutions (A) that need to be considered may therefore be written in the form

$$s_1^{mx}\, t_1,$$

where $x = 0, 1, \ldots\ldots, p-1$. These may evidently be replaced by the substitutions

$$(s_1 s_p \ldots\ldots s_{p-x+2})^m\, t_1,$$

where s_{p-x+2} stands for unity when $x = 0$ and for s_1 when $x = 1$. Now by the method used above (§10) it follows that the groups corresponding to the values $x = 1,\ 2, \ldots\ldots,\ p-1$ are conjugate. Hence in this case there are two groups that correspond to P_{p-1}.

The $q-1$ sets of substitutions that transform according to p_2 result when the head is multiplied by the substitutions

$$s_1^{\beta}\, t_2, \tag{A$_1$}$$

where $\beta = 0, 1, \ldots\ldots, q-2$. Each of these transforms the head and also $\{H, t_1\}$ into themselves. The $\dfrac{p-1}{i_2}$th power of (A_1) will be in the head if β satisfies the relation

$$\beta\left(\frac{p-1}{i}\right) \equiv 0 \qquad (\mathrm{mod}\ q-1). \tag{2}$$

To each value of β that satisfies this congruence there corresponds a distinct group that corresponds to P_{i_2} $(i_2 < p-1)$ and that contains $\{H,\ t_1\}$ as an invariant subgroup.

If $\{H,\ s_1^m\, t_1\}$ is contained as an invariant subgroup in a group that corresponds to P_{i_2}, then the former group must include the substitution

$$t_2^{-1}\, s_1^{-\beta}\, (s_1^m\, t_1)\, s_1^{\beta}\, t_2 = s_1^{m-\beta}\, s_r^{\beta}\, t_1^{\gamma},$$

where β satisfies the congruence (2) and r denotes one of the numbers $2, 3 \ldots\ldots,$ $p-1$. The group $\{H,\ s_1^m\, t_1\}$ contains the substitution $s_1^{m-\beta}\, s_r^{\beta}\, t_1$. If it also contained $s_1^{m-\beta}\, s_r^{\beta}\, t_1^{\gamma}$, then the substitution $t_1^{\gamma-1}$ would be found in it. This, however, is not the case since γ is not congruent to unity modulus p.

13. THEOREM.—*When $p > 2$, there is just one imprimitive group of degree pq that contains the head.*

$$H \equiv \{G_1,\ G_2, \ldots\ldots,\ G_p\}_{\frac{q(q-1)}{2},\ \frac{q(q-1)}{2}, \ldots,\ \frac{q(q-1)}{2}}$$

and whose substitutions interchange the systems of intransitivity of H according to P_{t_2}. When $p = 2$, there are two such groups.

The largest group within which the given head is invariant without having its systems interchanged is $\{G_1, G_2, \ldots, G_p\}$. This is of order $[q(q-1)]^p$, while H is of order $\left[\frac{q(q-1)}{2}\right]^p \cdot 2$. There are accordingly 2^{p-1} sets of substitutions that permute according to each substitution in P_{t_2}. Those that transform according to p_1 may be obtained by multiplying the head by the substitutions

$$s_1^{a_1} s_2^{a_2} \ldots s_{p-1}^{a_{p-1}} t_1 \qquad \text{(A)}$$

where $a_1, a_2, \ldots, a_p = 0$ or 1. Each of these transforms the head into itself, and each has its p^{th} power in the head. It may be noted, first, that all of these substitutions whose p^{th} power gives rise to the same substitution in the head generate, with H, conjugate groups. For, let $a_1', a_2', \ldots, a_{p-1}'$ and $a_1'', a_2'', \ldots, a_{p-1}''$ be two sets of values that satisfy the congruence

$$a_1 + a_2 + \ldots + a_{p-1} \equiv a \qquad (\text{mod } q-1),$$

a being the exponent of the p^{th} power of the corresponding substitutions. The inverse of $s_2^{\beta_2} s_3^{\beta_3} \ldots s_p^{\beta_p}$ is a substitution that transforms $\{H, s_1^{a_1'} s_2^{a_2'} \ldots s_{p-1}^{a_{p-1}'} t_1\}$ into $\{H, s_1^{a_1''}, s_2^{a_2''} \ldots s_{p-1}^{a_{p-1}''} t_1\}$ providing

$$\beta_i = (a_1' + a_2' + \ldots + a_{i-1}') - (a_1'' + a_2'' + \ldots + a_{i-1}'').$$

Of the substitutions (A) we need consider then only the following:

$$t_1 \text{ and } s_1 s_2 \ldots s_x t_1,$$

where $x = 1, 2, \ldots, p-1$. It follows, by the method used above (§10), that the $p-1$ groups $\{H, s_1 s_2 \ldots s_x t_1\}$ where $x = 1, 2, \ldots, p-1$, are conjugate. We have yet to consider the groups $\{H, t_1\}$ and $\{H, s_1 t_1\}$. The head H contains the substitution $s_1^{2\gamma_1+1} s_2^{2\gamma_2+1} \ldots s_p^{2\gamma_p+1}$ where $\gamma_1, \gamma_2, \ldots, \gamma_p$ may be zero or any integer. Hence $\{H, s_1 t_1\}$ contains the substitution, $s_1^{2\gamma_1+2} s_2^{2\gamma_2+1} s_3^{2\gamma_3+1} \ldots s_p^{2\gamma_p+1}, t_1$. The p^{th} power of this will be identity if the γ's satisfy the congruence

$$2(\gamma_1 + \gamma_2 + \ldots + \gamma_p) + p + 1 \equiv 0 \qquad (\text{mod } q-1)$$

i. e,

$$\gamma_1 + \gamma_2 \ldots + \gamma_p = -\frac{p+1}{2} \qquad \left(\text{mod } \frac{q-1}{2}\right).$$

This evidently has a solution except where $p = 2$. Hence, where $p > 2$, the group $\{H, s_1 t_1\}$ contains a substitution of order p in the division in which $s_1 t_1$ occurs. In this case, the groups $\{H, t_1\}$ and $\{H, s_1 t_1\}$ are clearly conjugate. When $p = 2$, the group $\{H, s_1 t_1\}$ contains negative substitutions, while $\{H, t_1\}$ does not. Hence, when p is even, there are two groups with the given head that correspond to P_{p-1}, and when p is odd there is one such group.

The sets of substitutions that transform according to p_2 may be found by multiplying the head by the substitutions

$$s_2^{\alpha_2} s_3^{\alpha_3} \cdots\cdots s_p^{\alpha_p} \; t_2, \tag{B}$$

where $\alpha_2, \alpha_3, \ldots\ldots, \alpha_p = 0$ or 1. These all transform the head into itself. Now

$$t_2^{-1} s_2^{-\alpha_2} s_3^{-\alpha_3} \cdots\cdots s_p^{-\alpha_p} t_1 s_2^{\alpha_2} s_3^{\alpha_3} \cdots\cdots s_p^{\alpha_p} t_2 = s_1^{\alpha_2} s_{i_3}^{\alpha_3 - \alpha_2} s_{i_4}^{\alpha_4 - \alpha_3} \cdots\cdots s_{i_{p-1}}^{\alpha_p - \alpha_{p-1}} s_{i_p}^{\alpha_p} t_1^{\gamma} \tag{C}$$

where $i_2, i_3, \ldots\ldots i_p = 2, 3, \ldots\ldots, p$ in some order and $t_2^{-1} t_1 t_2 = t_1^{\gamma}$. Since $\alpha_2, \ldots\ldots, \alpha_p = 0$ or 1, it follows that the exponents of the s's that precede t_1^{γ} are either 0, 1, or -1. Further if (C) is found in $\{H, t_1\}$ when the exponent of one of the s's is zero they must all be zero. It follows that $\alpha_2 = \alpha_3 = \ldots\ldots = \alpha_p = 0$ is the only set of values which give a substitution (B) that transforms $\{H, t_1\}$ into itself. Hence there is just one group that contains the given head and corresponds to P_{i_2} when i_2 is less than $p - 1$.

14. THEOREM.—*When* $p > 2$ *and* $\frac{p-1}{i_2}$ *is even there are two imprimitive groups that contain the head*

$$H \equiv \{G_1, G_2, \ldots\ldots, G_p\} \text{ pos},$$

and whose substitutions interchange the systems of intransitivity of H *according to* P_{i_2}; *when* $\frac{p-1}{i_2}$ *is odd there is just one such group. When* $p = 2$ *there are two groups that contain the given head.*

15. The heads considered in paragraphs 8–14 occur for all values of q and hence the theorems proved enable us to determine certain imprimitive groups of every degree of the form pq. In general, other intransitive groups can be formed from the p transitive groups $G_{1, t_1}, G_{2, t_1}, \ldots\ldots, G_{p, t_1}$ which may be used as heads of imprimitive groups whose systems of imprimitivity are permuted according to P_{i_2}. For each such head a like theorem may be proved.

SECTION IV. *List of the imprimitive groups of degree fifteen.*

The theorems proved in the preceding section enable us to find at once most of the imprimitive groups of the degrees four, six, nine, ten, and fourteen. We shall now make use of them in determining the imprimitive groups of degree fifteen.

Fifteen letters can be divided in two ways into systems containing an equal number of letters, viz., into three systems of five letters each, or into five systems of three letters each. We consider first the groups that contain three systems of imprimitivity. The substitutions of these groups permute the systems according to either the symmetric group or the alternating group of degree three. It follows that any intransitive group of degree fifteen that can be used as the head of such a group must permit a cyclic interchange of its systems of intransitivity. It is not difficult to construct all the intransitive groups of degree fifteen having three systems of intransitivity that have this property. It is found that there are twenty-one such groups which can be used as heads. They are as follows:

Order.	
1728000	$(abcde)$ all $(fghij)$ all $(klmno)$ all
864000	$\{(abcde)$ all $(fghij)$ all $(klmno)$ all$\}$ pos
432000	$(abcde)$ pos $(fghij)$ pos $(klmno)$ pos $+$
	$(abcde)$ neg $(fghij)$ neg $(klmno)$ neg
216000	$(abcde)$ pos $(fghij)$ pos $(klmno)$ pos
8000	$(abcde)_{20}\,(fghij)_{20}\,(klmno)_{20}$
4000	$\{(abcde)_{20}\,(fghij)_{20}\,(klmno)_{20}\}$ pos
2000	$[\{(abcde)_{20}\,(fghij)_{20}\}$ pos, $(klmno)_{20}]$ dim
2000	$\{(abcde)_{20}\,(fghij)_{20},\,(klmno)_{20}\}_{100,\,5}$
1000	$(abcde)_{10}\,(fghij)_{10}\,(klmno)_{10}$
500	$\{(abcde)_{20}\,(fghij)_{20}\,(klmno)_{20}\}_{5,\,5,\,5}$
500	$\{(abcde)_{10}\,(fghij)_{10},\,(klmno)_{10}\}$ dim
250	$\{(abcde)_{10}\,(fghij)_{10}\,(klmno)_{10}\}_{5,\,5,\,5}$
125	$(abcde)_{5}\,(fghij)_{5}\,(klmno)_{5}$
120	$(abcde\,.\,fghij\,.\,klmno)_{120}$
100	$[\{(abcde)_{20}\,(fghij)_{20}\}_{5,\,5},\,(klmno)_{20}]_{5,\,1}$
60	$(abcde\,.\,fghij\,.\,klmno)_{60}$
50	$[\{(abcde)_{10}\,(fghij)_{10}\}$ dim, $(klmno)_{10}]_{5,\,1}$

25 $\{(abcde)_5\,(fghij)_5,\,(klmno)\}_{5,\,1}$
20 $(abcde\,.\,fghij\,.\,klmno)_{20}$
10 $(abcde\,.\,fghij\,.\,klmno)_{10}$
5 $(abcde\,.\,fghij\,.\,klmno)_5$

The theorems of the preceding section enable us to write down at once all of the imprimitive groups that have the above groups for heads except the second head of order 500. It is easily found that there are three groups that contain this head. The total number of these is found to be 55 and they may be written as follows:

Order.	No.	
10368000	1	$(abcde)$ all $(fghij)$ all $(klmno)$ all $(afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)$ $(af\,.\,bg\,.\,ch\,.\,di\,.\,ej)$
5184000	1	$(abcde)$ all $(fghij)$ all $(klmno)$ all $(afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)$
	2, 3	$\{(abcde)$ all $(fghij)$ all $(klmno)$ all$\}$ pos $(afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)(af\,.\,bg\,.\,ch\,.\,di\,.\,ej)(1,\,ab)$
2592000	1	$\{(abcde)$ all $(fghij)$ all $(klmno)$ all$\}$ pos $(afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)$
2592000	2	$(abcde)$ pos $(fghij)$ pos $(klmno)$ pos $+$ $(abcde)$ neg $(fghij)$ neg $(klmno)$ neg $(afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)(af\,.\,bg\,.\,ch\,.\,di\,.\,ej)$
1296000	1	$\{(abcde)$ pos $(fghij)$ pos $(klmno)$ pos $+$ $(abcde)$ neg $(fghij)$ neg $(klmno)$ neg$\}$ $(afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)$
	2, 3	$(abcde)$ pos $(fghij)$ pos $(klmno)$ pos $(afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)$ $(af\,.\,bg\,.\,ch\,.\,di\,.\,ej)(1,\,ab\,.\,fg\,.\,kl)$
648000	1	$(abcde)$ pos $(fghij)$ pos $(klmno)$ pos $(afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)$
48000	1	$(abcde)_{20}\,(fghij)_{20}\,(klmno)_{20}\,(afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)$ $(af\,.\,bg\,.\,ch\,.\,di\,.\,ej)$
24000	1	$(abcde)_{20}\,(fghij)_{20}\,(klmno)_{20}\,(afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)$
	2	$\{(abcde)_{20}\,(fghij)_{20}\,(klmno)_{20}\}$ pos $(afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)$ $(af\,.\,bg\,.\,ch\,.\,di\,.\,ej)$
	3	$\{(abcde)_{20}\,(fghij)_{20}\,(klmno)_{20}\}$ pos $(afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)$ $(bced)(af\,.\,bg\,.\,ch\,.\,di\,.\,ej)$
12000	1	$\{(abcde)_{20}\,(fghij)_{20}\,(klmno)_{20}\}$ pos $(afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)$
	2	$[\{(abcde)_{20}\,(fghij)_{20}\}$ pos, $(klmno)_{20}]$ dim $(afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)(af\,.\,bg\,.\,ch\,.\,di\,.\,ej)$

12000	3, 4	$\{(abcde)_{20}\,(fghij)_{20},\,(klmno)_{20}\}_{100,\,5}\,(afk.bgl.chm.din.ejo)$
		$(af.bg.ch.di.ej)(1,\,lo.mn)$
6000	1	$[\{(abcde)_{20}\,(fghij)_{20}\}\ \text{pos},\,(klmno_{20})]\ \text{dim}\ (afk.bgl.chm.din.ejo)$
	2	$\{(abcde)_{20}\,(fghij)^{20},\,(klmno)_{20}\}_{100,\,5}\,(afk.bgl.chm.din.ejo)$
	3, 4	$(abcde)_{10}\,(fghij)_{10}\,(klmno)_{10}\,(afk.bgl.chm.din.ejo)$
		$(af.bg.ch.di.ej)(1,\,bced.ghji.lmon)$
3000	1	$(abcde)_{10}\,(fghij)_{10}\,(klmno)_{10}\,(afk.bgl.chm.din.ejo)$
	2	$\{(abcde)_{20}\,(fghij)_{20}\,(klmno)_{20}\}_{5,\,5,\,5}\,(afk.bgl.chm.din.ejo)$
		$(af.bg.ch.di.ej)$
	3, 4	$\{(abcde)_{10}\,(fghij)_{10},\,(klmno)_{10}\}\ \text{dim}\ (afk.bgl.chm.din.ejo)$
		$(af.bg.ch.di.ej)(1,\,be.cd)$
1500	1	$\{(abcde)_{20}\,(fghij)_{20}\,(klmno)_{20}\}_{5,\,5,\,5}\,(afk.bgl.chm.din.ejo)$
	2	$\{(abcde)_{10}\,(fghij)_{10},\,(klmno)_{10}\}\ \text{dim}\ (afk.bgl.chm.din.ejo)$
	3, 4	$\{(abcde)_{10}\,(fghij)_{10}\,(klmno)_{10}\}_{5,\,5,\,5}\,(afk.bgl.chm.din.ejo)$
		$(af.bg.ch.di.ej)(1,\,bced.ghji.lmon)$
750	1	$\{(abcde)_{10}\,(fghij)_{10}\,(klmno)_{10}\}_{5,\,5,\,5}\,(afk.bgl.chm.din.ejo)$
	2, 3	$(abcde)_{5}\,(fghij)_{5}\,(klmno)_{5}\,(afk.bgl.chm.din.ejo)$
		$(af.bg.ch.di.ej)(1,\,be.cd.gj.hi.lo.mn)$
720	1	$*(abcde.fghij.klmno)_{120}\,(afk.bgl.chm.din.ejo)(af.bg.ch.di.ej)$
600	1	$[\{(abcde)_{20}\,(fghij)_{20}\}_{5,\,5},\,(klmno)_{20}]_{5,\,1}\,(afk.bgl.chm.din.ejo)$
		$(af.bg.ch.di.ej)$
375	1	$(abcde)_{5}\,(fghij)_{5}\,(klmno)_{5}\,(afk.bgl.chm.din.ejo)$
360	1	$*(abcde.fghij.klmno)_{120}\,(afk.bgl.chm.din.ejo)$
	2, 3	$*(abcde.fghij.klmno)_{60}\,(afk.bgl.chm.din.ejo)$
		$(af.bg.ch.di.ej)(1,\,ab.fg.kl)$
300	1	$[\{(abcde)_{20}\,(fghij)_{20}\}_{5,\,5}\,(klmno)_{20}]_{5,\,1}\,(afk.bgl.chm.din.ejo)$
	2, 3	$[\{(abcde)_{10}\,(fghij)_{10}\}\ \text{dim},\,(klmno)_{10}]_{5,\,1}\,(afk.bgl.chm.din.ejo)$
		$(af.bg.ch.di.ej)(1,\,bced.ghji.lmon)$
180	1	$*(abcde.fghij.klmno)_{60}\,(afk.bgl.chm.din.ejo)$
150	1	$[\{(abcde)_{10}\,(fghij)_{10}\}\ \text{dim},\,(klmno)_{10}]_{5,\,1}\,(afk.bgl.chm.din.ejo)$
	2, 3	$\{(abcde)_{5}\,(fohij)_{5},\,(klmno)_{5}\}_{5,\,1}\,(afk.bgl.chm.din.ejo)$
		$(af.bg.ch.di.ej)(1,\,be.cd.gj.hi.lo.mn)$
120	1	$*(abcde.fghij.klmno)_{20}\,(afk.bgl.chm.din.ejo)$
		$(af.bg.ch.di.ej)$

75	1	$\{(abcde)_5\ (fghij)_5,\ (klmno)_5\}_{5,\,1}\ (afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)$
60	1	$*(abcde\,.\,fghij\,.\,klmno)_{20}\ (afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)$
	2, 3	$*(abcde\,.\,fghij\,.\,klmno)_{10}\ (afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)$ $(af\,.\,bg\,.\,ch\,.\,di\,.\,ej)(1,\ bced\,.\,ghji\,.\,lmon)$
30	1	$*(abcde\,.\,fghij\,.\,klmno)_{10}\ (afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)$
	2, 3	$*(abcde\,.\,fghij\,.\,klmno)_5\ (afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)$ $(af\,.\,bg\,.\,ch\,.\,di\,.\,ej)(1,\ be\,.\,cd\,.\,gj\,.\,hi\,.\,lo\,.\,mn)$
15	1	$*(abcde\,.\,fghij\,.\,klmno)_5\ (afk\,.\,bgl\,.\,chm\,.\,din\,.\,ejo)$
Total,	55	

Those groups marked with an * have also five systems of imprimitivity.

The symmetric group and the alternating group of degree five can each be represented as an imprimitive group of degree fifteen. Hence identity occurs among the heads of the imprimitive groups of degree fifteen that have five systems of imprimitivity. The transitive constituents of the other heads of these groups are cyclic groups of order three or symmetric groups of order six. And as in the preceding case each of these heads permits a cyclic interchange of its systems of intransitivity. It is found that there are nine groups that can be used for heads of imprimitive groups of degree fifteen that have five systems of imprimitivity. They are as follows:

Order.	
7776	(abc) all (def) all (ghi) all (jkl) all (mno) all
3888	$\{(abc)$ all (def) all (ghi) all (jkl) all (mno) all$\}$ pos
486	$\{(abc)$ all (def) all (ghi) all (jkl) all (mno) all$\}_{3,\,3,\,3,\,3,\,3}$
243	$(abc)(def)(ghi)(jkl)(mno)$
162	$(abc\,.\,dfe)(def\,.\,gih)(ghi\,.\,jlk)(jkl\,.\,mon)(ab\,.\,de\,.\,gh\,.\,jk\,.\,mn)$
81	$(abc\,.\,dfe)(def\,.\,gih)(ghi\,.\,jlk)(jkl\,.\,mon)$
6	$(abc\,.\,def\,.\,ghi\,.\,jkl\,.\,mno)$ all
3	$(abc\,.\,def\,.\,ghi\,.\,jkl\,.\,mno)$ cyc
1	Identity

The theorems of the preceding section enable us to determine all the imprimitive groups that contain these heads except those whose substitutions interchange their systems of imprimitivity according to either the symmetric or the

alternating group of degree five. We note briefly the construction of the latter. Those that contain the head identity can be found at once by means of Dyck's theorem on the transitive representation of a given group.* The heads of orders 7776 and 6 are not contained in larger groups of the same degree that leave their systems of intransitivity unchanged. The groups that contain these heads and that correspond to $(abcde)$ all or $(abcde)$ pos are determined then at once.† The groups that contain the head of order 3 and that correspond to $(abcde)$ all or $(abcde)$ pos are of order 360 or 180 and their factors of composition are 60, 3, 2 and 60, 3 respectively. The abstract groups with these factors of composition are known,‡ and hence we can at once find the corresponding imprimitive groups. The remaining groups (12 in number) may be easily found by tentative processes.

I find in all 56 distinct groups that contain five systems of imprimitivity. Of these, 13 have also three systems of imprimitivity and so are found in the preceding list. Those which contain five systems of imprimitivity without also containing three systems are the following:

Order	No.	
933120	1	(abc) all (def) all (ghi) all (jkl) all (mno) all
		$(adgjm \,.\, behkn \,.\, cfilo)(ad \,.\, be \,.\, cf)$
466560	1	(abc) all (def) all (ghi) all (jkl) all (mno) all
		$(adgjm \,.\, behkn \,.\, cfilo)(adg \,.\, beh \,.\, cfi)$
	2, 3	$\{(abc)$ all (def) all (ghi) all (jkl) all (mno) all$\}$ pos
		$(adgjm \,.\, behkn \,.\, cfilo)(ad \,.\, be \,.\, cf)(1, gh)$
233280	1	$\{(abc)$ all (def) all (ghi) all (jkl) all (mno) all$\}$ pos
		$(adgjm \,.\, behkn \,.\, cfilo)(adg \,.\, beh \,.\, cfi)$
155520	1	(abc) all (def) all (ghi) all (jkl) all (mno) all
		$(adgjm \,.\, behkn \,.\, cfilo)(dgmj \,.\, ehnk \,.\, fiol)$
77760	1	(abc) all (def) all (ghi) all (jkl) all (mno) all
		$(adgjm \,.\, behkn \,.\, cfilo)(dm \,.\, gj \,.\, en \,.\, hk \,.\, fo \,.\, il)$
	2, 3	$\{(abc)$ all (def) all (ghi) all (jkl) all (mno) all$\}$ pos
		$(adgjm \,.\, behkn \,.\, cfilo)(dgmj \,.\, ehnk \,.\, fiol)(1, ab)$

* Mathematische Annalen, Vol. 22 (1883), p. 94.

† Miller, Quarterly Journal of Mathematics, Vol. 28 (1895), p. 195.

‡ Hölder, Mathematische Annalen, Vol. 46 (1895), p. 417.

58320	1	{(*abc*) all (*def*) all (*ghi*) all (*jkl*) all (*mno*) all}$_{3, 3, 3, 3, 3,}$ (*adgjm* . *behkn* . *cfilo*)(*ad* . *be* . *cf*)
38880	1	(*abc*) all (*def*) all (*ghi*) all (*jkl*) all (*mno*) all (*adgjm* . *behkn* . *cfilo*)
	2, 3	{(*abc*) all (*def*) all (*ghi*) all (*jkl*) all (*mno*) all} pos (*adgjm* . *behkn* . *cfilo*)(*dm* . *gj* . *en* . *hk* . *fo* . *il*)(1, *ab*)
29160	1	{(*abc*) all (*def*) all (*ghi*) all (*jkl*) all (*mno*) all}$_{3, 3, 3, 3, 3}$ (*adgjm* . *behkn* . *cfilo*)(*adg* . *beh* . *cfi*)
	2, 3	(*abc*)(*def*)(*ghi*)(*jkl*)(*mno*)(*adgjm* . *behkn* . *cfilo*) (*ad* . *be* . *cf*)(1, *ab* . *de* . *gh* . *jk* . *mn*)
19440	1	{(*abc*) all (*def*) all (*ghi*) all (*jkl*) all (*mno*) all} pos (*adgjm* . *behkn* . *cfilo*)
	2	(*abc* . *dfe*)(*def* . *gih*)(*ghi* . *jlk*)(*jkl* . *mon*)(*ab* . *de* . *gh* . *jk* . *mn*) (*adgjm* . *behkn* . *cfilo*)(*ad* . *be* . *cf*)
14580	1	(*abc*)(*def*)(*ghi*)(*jkl*)(*mno*)(*adgjm* . *behkn* : *cfilo*)(*adg* . *beh* . *cfi*)
9720	1	{(*abc*) all (*def*) all (*ghi*) all (*jkl*) all (*mno*) all}$_{3, 3, 3, 3, 3}$ (*adgjm* . *behkn* . *cfilo*)(*dgmj* . *ehnk* . *fiol*)
	2	(*abc* . *dfe*)(*def* . *gih*)(*ghi* . *jlk*)(*jkl* . *mon*)(*ab* . *de* . *gh* . *jk* . *mn*) (*adgjm* . *behkn* . *cfilo*)(*adg* . *beh* . *cfi*)
	3, 4	(*abc* . *dfe*)(*def* . *gih*)(*ghi* . *jlk*)(*jkl* . *mon*)(*adgjm* . *behkn* . *cfilo*) (*ad* . *be* . *cf*)(1, *ab* . *de* . *gh* . *jk* . *mn*)
4860	1	{(*abc*) all (*def*) all (*ghi*) all (*jkl*) all (*mno*) all}$_{3, 3, 3, 3, 3}$ (*adgjm* . *behkn* . *cfilo*)(*dm* . *gj* . *en* . *hk* . *fo* . *il*)
	2, 3	(*abc*)(*def*)(*ghi*)(*jkl*)(*mno*)(*adgjm* . *behkn* . *cfilo*) (*dgmj* . *ehnk* . *fiol*)(1, *ab* . *de* . *gh* . *jk* . *mn*)
	4	(*abc* . *dfe*)(*def* . *gih*)(*ghi* . *jlk*)(*jkl* . *mon*)(*adgjm* . *behkn* . *cfilo*) (*adg* . *beh* . *cfi*)
3240	1	(*abc* . *dfe*)(*def* . *gih*)(*ghi* . *jlk*)(*jkl* . *mon*)(*ab* . *de* . *gh* . *jk* . *mn*) (*adgjm* . *behkn* . *cfilo*)(*dgmj* . *ehnk* . *fiol*)
2430	1	{(*abc*) all (*def*) all (*ghi*) all (*jkl*) all (*mno*) all}$_{3, 3, 3, 3, 3}$ (*adgjm* . *behkn* . *cfilo*)
	2, 3	(*abc*)(*def*)(*ghi*)(*jkl*)(*mno*)(*adgjm* . *behkn* . *cfilo*) (*dm* . *gj* . *en* . *hk* . *fo* . *il*)(1, *ab* . *de* . *gh* . *jk* . *mn*)
1620	1	(*abc* . *dfe*)(*def* . *gih*)(*ghi* . *jlk*)(*jkl* . *mon*)(*ab* . *de* . *gh* . *jk* . *mn*) (*adgjm* . *behkn* . *cfilo*)(*dm* . *gj* . *en* . *hk* . *fo* . *il*)

1620,	3	(abc . dfe)(def . gih)(ghi . jlk)(jkl . mon)(adgjm . behkn . cfilo) (dgmj . ehnk . fiol)(1, ab . de . gh . jk . mn)
1215	1	(abc)(def)(ghi)(jkl)(mno)(adgjm . behkn . cfilo)
810	1	(abc . dfe)(def . gih)(ghi . jlk)(jkl . mon)(ab . de . gh . jk . mn) (adgjm . behkn . cfilo)
	2, 3	(abc . dfe)(def . gih)(ghi . jlk)(jkl . mon)(adgjm . behkn . cfilo) (dm . gj . en . hk . fo . il)(1, ab . de . gh . jk . mn)
405	1	(abc . dfe)(def . gih)(ghi . jlk)(jkl . mon)(adgjm . behkn . cfilo)
360	1	(abc . def . ghi . jkl . mno) cyc (adgjm . behkn . cfilo) (def . gkn . hlo , ijm)
180	1	(abc . def . ghi . jkl . mno) cyc (adgjm . behkn . cfilo) (aeh . bfi . cdg . mno)
120	1	(adgjm . behkn . cfilo)(ad . be . cf)
60	1	(adgjm . behkn . cfilo)(adg . beh . cfi)
	43	

CORNELL UNIVERSITY, *June*, 1901.